

CONTINUOUS MONITORING OF RISKS – PEOPLE, PLANT AND PROCESS

Dr. John Bond

The aviation industry has demonstrated that the flight hazards associated with the operation of large public transport aircraft can be monitored and the recognised risks controlled to improve safety significantly. They have introduced this new approach with:-

- Flight data monitoring and analysis covering people, equipment and operating conditions.
- Just Culture.
- Sharing information.

This approach has had the active support of the Civil Aviation Authority and the Air Accident Investigation Branch and makes the approach less error prone and more error aware. Its objective is not to decrease the safety accountability of the operator but to increase the safety accountability of everyone who designs, constructs, manages, operates and maintains the system.

The paper will describe ways that this approach can be applied to computer controlled petrochemical plants to monitor all the identified hazards, to analyse the operation against the limits set in operating procedures and hence provide information to control risks on a continuous basis and to improve safety.

KEYWORDS: Monitoring risks; Just Culture; risk control; evolutionary management.

INTRODUCTION

Accidents usually occur when a series of errors in the equipment, in the process or in the method of operation coincide. Seldom does a single error result in an accident. If the people, the equipment and the process are monitored the data obtained can be used to identify errors that occur and hence establish the level of the risk involved in the whole operation. Once the frequency of errors is established then they can be addressed, the process altered and the new level of risk established. The production activity thus incorporates the provision of information for the improvement in safety. This evolutionary management system becomes a dynamic and progressive philosophy leading to reduced risk all round.

The recent report on the Texas Refinery Fire (BAKER 2007) produced a number of recommendations and under the section "*Measuring process safety performance*" it states "As a result, BP's corporate safety management system for its U.S. refineries does not effectively measure and monitor process safety performance" Thus Recommendation 2

titled "INTEGRATED AND COMPREHENSIVE PROCESS SAFETY MANAGEMENT SYSTEM" required:-

> " BP should establish and implement an integrated and comprehensive process safety management system that systematically and continuously identifies, reduces, and manages process safety risks at its U.S. refineries."

I suspect that these criticisms apply equally to many companies, but what is a comprehensive process safety management system? I am sure that there is much debate about what it comprises but I would expect it to start at the top of the company with a corporate:-

- statement on leadership and responsibility at all levels of the organisation;
- requirement to comply with all management systems; and
- development plan for a safety culture that was just, identified hazards and monitored the risk arising from the personnel, plant and process.

The Buncefield Standards Task Group Final Report (HSE 2007) requires an active monitoring operation of tank storage but makes no mention of direct monitoring of operator's work.

It is my view that a system of monitoring all the identified hazards in a process operation (equipment, process and personnel) to ensure that the risks are under control to an acceptable level is now required. Any variation of the operation from the finalised Standard Operating Procedures (SOP) would be noted and a prompt decision made whether to alter the SOP, carry out maintenance of the equipment or provide additional training as appropriate. This would provide the demonstrated control of the risks involved that is required by the Baker Report (BAKER 2007).

THE AVIATION INDUSTRY

The civil aviation industry has introduced over recent years a comprehensive method of monitoring the operational flying standards of large civil airliners. This includes the monitoring of identified hazards involved in each flight operation, the analysis of the data against the boundaries set in the Standard Operating Procedures (SOP) for the flight, a Just Culture approach and a sharing of information on accidents and near-miss events. As a result they have knowledge of and are in control of all the identified risks involved in the flight operations. Any modification of the SOPs can be studied in following flights to ensure that the risk has been reduced. This management system has been so successful that it is now being applied to helicopters (CAA 2002).

The Flight Data Monitoring system (CAA 2003) (see Figures 1, 2 and 3) records data on the crew's operational performance, the performance of the equipment and the flight conditions for each flight. The data is removed after the flight by a disc or by telemetry and analysed. In British Airways this is done automatically by the Special Event Search and Master Analysis (SESMA) software which can evaluate the whole flight against the

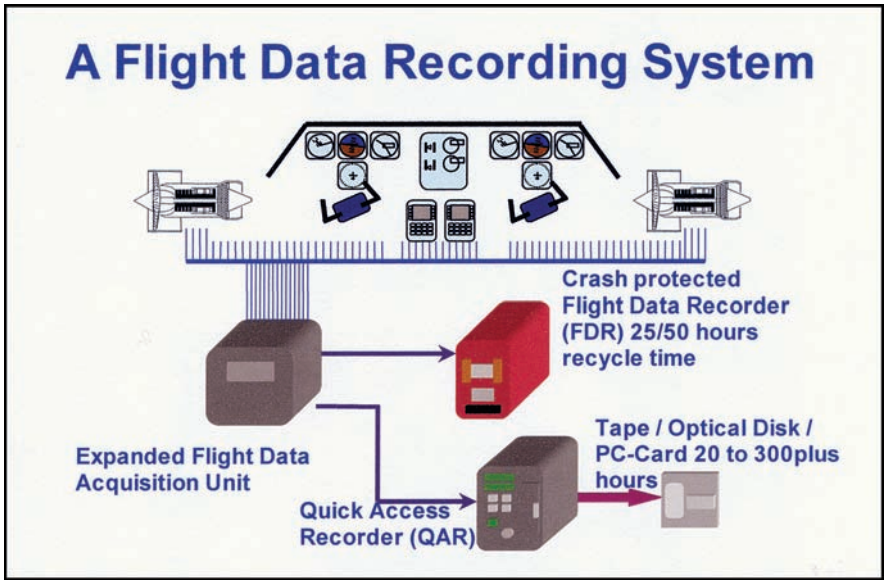

Figure 1. (CAA 2003)

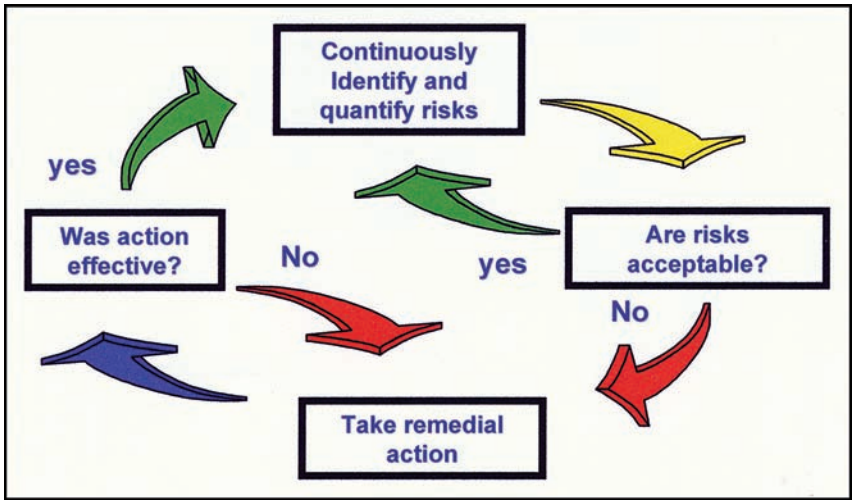

Figure 2. (CAA 2003)

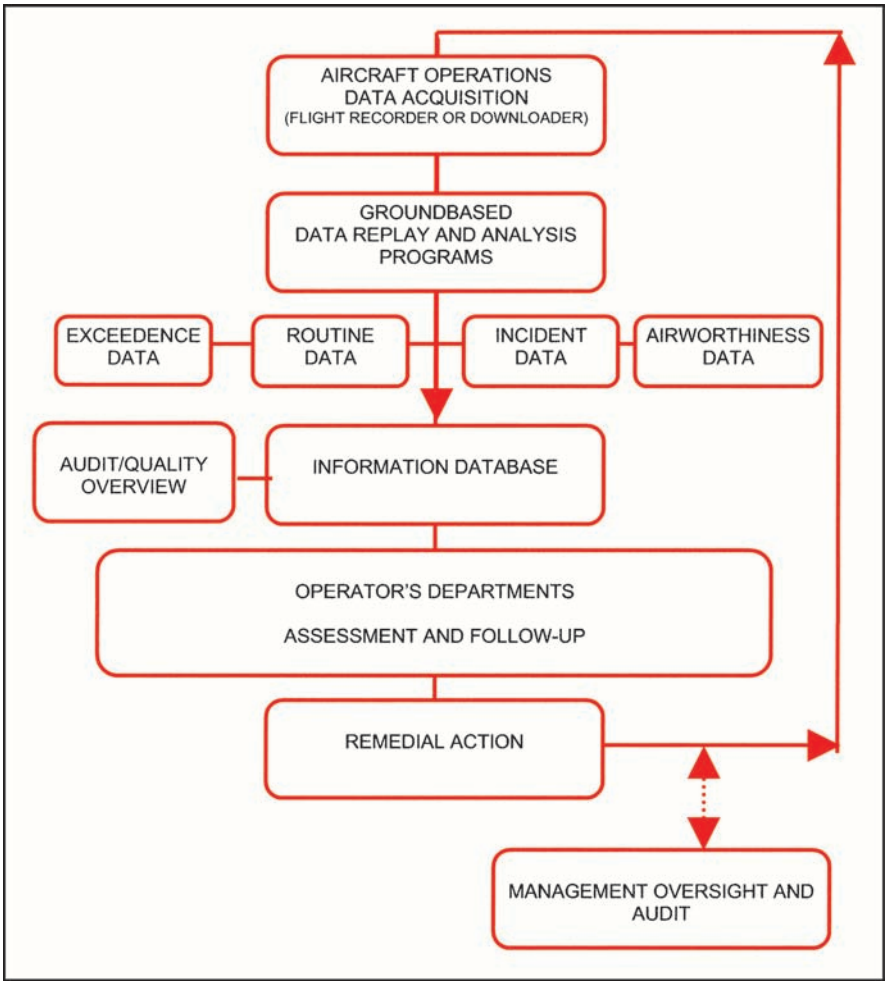

Figure 3. (CAA 2003)

SOPs and records any data that exceeds the limits set. Output from the analysis can automatically show:-

- Compliance with operating procedures by the crew and can feed this if necessary into training programmes
- The state of the equipment and can feed this information into maintenance programmes.

- Flight operating conditions for unusual flight conditions to be studied by appropriate personnel.

The Civil Aviation Authority defines (CAA 2003) the Flight Data Monitoring as a "*… systematic, pro-active and non-punitive use of digital flight data from routine operations to improve aviation safety.*"

The choice of data to be collected is based on the identified hazards involved in the operation and could be described as a study of hazards and operability similar to a HAZOP. Each operator configures his Flight Data Monitoring programme to reflect his SOPs and any exceedence of the boundaries set is identified by the SESMA system. These are then noted and appropriate action taken to ensure safety of operations. This ensures that all the risks are continuously monitored and their level evaluated and reduced where necessary. The whole process becomes an evolutionary management system which monitors and reduces the risk of flight operation.

The monitoring of the pilot operations on an airliner in the UK covers a wide variety of some 100 plus conditions such as climbing speed too low, flaps out speed exceeds limit set in SOP, too deep landing, tail scrape and many others. About 400 to 500 events each month are discovered, usually only minor infringements of the limits but some more serious resulting in 10 to 20 crews being contacted for an explanation. The pilot's union are involved as middlemen in these discussions and hence confidentiality maintained.

The Flight Data Monitoring system thus provides information on the level of risk of each identified hazard and provides information both within the aircraft and external e.g. weather, Air Traffic Control, Airport.

The Just Culture approach was found to be a necessary part of the Flight Data Monitoring system as it involved the work of the crew. In rejecting the blame culture, the International Civil Aviation Organisation (ICAO), states in Section 4.5.40 of Safety Management Manual (ICAO 2006):

> *"If an accident was the result of an error in judgement or technique, it is almost impossible to effectively punish for that error. …… If punishment is selected in such cases, two outcomes are almost certain. Firstly, no further reports will be received of such errors. Secondly, since nothing has been done to change the situation, the same accident could be expected again."*

A Just Culture has been defined (GLOBAL 2004) as:

> *"A way of thinking that promotes a questioning attitude, is resistant to complacency, is committed to excellence, and fosters both personal accountability and corporate self-regulation in safety matters."*

The approach has been described by James Reason (REASON 1998 and 2005) and has been applied also in the Air Traffic Management area of the aviation industry to improve safety. He states that:

> *"A prerequisite for a just culture is that all members of an organisation should understand where the line must be drawn between unacceptable behaviour,*

> *deserving of disciplinary action, and the remainder, where punishment is neither appropriate nor helpful in furthering the cause of safety".*

The civil aviation industry also has two major information systems to share information and lessons learnt comprising the Mandatory Occurrence Reporting Scheme (MORS) and the Confidential Human Incident Reporting Programme (CHIRP). It is for the adoption of these approaches to safety that the Just Culture becomes important.

The civil aviation industry in Australia, Canada and the UK has fully adopted the management system involving all three approaches:

- Flight Data Monitoring system with continuous analysis.
- The Just Culture approach.
- The sharing of accident and near-miss information

This has resulted in an increase in the reporting of incidents while keeping low the fatal accident rate. The fatal accident rate (fatalities per million hours flight) over a period of ten years for UK Registered/operated Large Public Transport Aeroplanes (3 year moving average) was only 5 fatal accidents causing 8 fatalities over the ten year period. Australia, Canada and the UK currently have a 3 year moving average fatal accident rate of zero compared with a figure of 13 for the whole world. These figures are based on Western designed aircraft with similar training courses but different management and regulatory systems

This approach to controlling the risks involved may not be directly applicable to other industries but the principles of:

- Monitoring the identified hazards associated with personnel, equipment and conditions on the flight, analysing the data against the limits set in the SOP and hence identifying the level of risk in the operation.
- Setting up a Just Culture approach to ensure the sharing of information
- Sharing information with other companies

are applicable to many other industries. The three stages are interdependent with one another to get the full value of the risk minimising process.

The difficulty of obtaining acceptance by the work force is much more of a problem if they are not brought into the process. As with civil aviation staff the consequences of errors by process operating staff can result in fatalities and therefore both staff and management have an interest in reducing risk. In the UK civil aviation industry the pilots union are an integral part of the safety culture.

This approach in the civil aviation industry was spearheaded by the ICAO, the CAA, the AAIB, the European Commission, Eurocontrol and the companies who have all taken an active part in its development. It is not surprising that Lord Broers, Past President of the Royal Academy of Engineering stated (BROERS 2005):

> *"One crucial recommendation emerges* (from the debate in the Royal Academy of Engineering). *That the investigation of accidents should concentrate on finding the cause of the accidents not the person or persons to blame. The latter*

only leads to defensiveness and cover up. The investigation should seek the cause of the accident so that it may be eliminated in the future. The airline industry's remarkable safety record is thought by some to be because the investigators seek the cause of accidents rather than hunt down the person to blame."

MONITORING AND ANALYSIS IN THE PROCESS INDUSTRIES

The design of plant is now always subjected to a HAZOP study where the hazards are identified and the risks assessed. Modifications to the design are then made to ensure an acceptable level of risk. Monitoring of the risks during operation is based on well recognised standards. Equipment is inspected on a schedule dependant upon experience and records are kept of all equipment. Instrumentation is tested on a regular basis and also recorded. However, corrosion of equipment causes a number of serious accidents and online monitoring of pipework for corrosion is needed.

The hazards of the process are also well established prior to design and are kept in mind at the HAZOP stage and suitably dealt with. The process is monitored continuously to ensure that the right product is produced and in an efficient manner.

The hazards associated with people making an operational error are not always dealt with sufficiently. It is assumed that the training and competency assessment would prevent most errors. Monitoring of process operators is carried out by the supervision provided.

Continuous monitoring by computer of risks associated with the process operators, the plant equipment and the process is possible on the larger plants and has been shown to be very effective in the aviation industry. It should be applied in the process industry and could begin with the start-up operations, extended through the whole of the process operation and with the shut down operations

Establishing the finalised SOP is an opportunity to ensure that all of the identified hazards are monitored on a continuing basis. Analysis of the data obtained during operation of the process will:-

- Identify and quantify operational risks associated with the people, the plant and the process on a continuous basis;
- Identify and quantify any changing risks in the operational work;
- Formally assess the risks to determine which are not at an acceptable level;
- Where the risks are not acceptable take remedial actions;
- Demonstrate that the risks are being monitored continuously;
- Provide leading safety performance measurements as indicators.

The whole monitoring programme and analysis becomes an evolutionary safety management system to reduce risk and provide improvements in the level of safety.

MONITORING OF PROCESS OPERATORS

Continuous monitoring of process operators was frowned upon by the unions because of the attitude to 'blame the operator' which would lead to disciplinary measures. If the blame

culture was completely removed from the monitoring process, the advantage in safety could be demonstrated bearing in mind it is the operator that is the one usually injured in an accident. Such a monitoring operation was carried out (BOND 1975) when random sampling of operators and craftsmen was used to see if all of the operations were being carried out to the SOP. All process and maintenance operations were defined with two safeguards being required to protect the men against all reasonably foreseeable hazards. Activity Sampling was carried out on a random basis to establish what the true position was based on a 95% confidence limit. This work was carried out with the knowledge and support of the unions on the understanding that no names would be recorded on any sample taken. Hence there was no blame associated with the procedure. It was found that compliance with the SOP after the first training period was 78% for operators and 54% for craftsmen. After further training the compliance was raised to 79% and 73% respectively. The training of the men and the random sampling were unfortunately stopped not by the unions but by senior management! My experience of monitoring process operators and craftsmen was that there were relatively few problems if the reasons were made clear and if it was explained that you were honestly not seeking anyone to blame.

In the past the work of process operators running process plant was monitored by foremen, chargehands and senior operators. With the reduction of supervision people there has been a greater reliance on human factors including training and competency of the operators. This is important but, as with pilots, operators are human and can make occasional errors. When errors do occur investigations usually show that there has been an operation outside the limits set in the SOP. The training or competency process is then usually blamed.

With the computer control of process operations the monitoring of process operators would be possible particularly for start-up, normal operations, shut down and emergency procedures. The following operations would be critical operating parameters affecting safety and could be monitored:

Start-up Procedure where errors occur:

- Correct sequence of start-up
- Valves in correct position
- Flow conditions correct
- Alarms commissioned
- Compressors operating satisfactorily
- Thermal shock due to heating up too fast

Normal Operations where errors occur:

- Reliance on high level alarms to stop transfer operations to tanks
- Alarms failed to be back on line after testing
- Alarm isolations, response and reinstalling
- Relief valves lifting due to pressure resulting from the temperature of the LPG being pumped into the tank is too high.
- Warning of temperature excursions

Consider just two examples, thermal shock and transfer to a tank.

Heating up of pipes and flanges at a maximum rate of, say, 25°C per hour as specified in the SOP, allows equality in the heating up process and maintains integrity of the system. If the heating up rate is exceeded there is a greater possibility of losing containment of material. The heating up rate of items could be continuously monitored and any that exceeds the specified rate set in the SOP would be noted. A very short and small excess

might be considered only a small risk but should be noted by the data analysis and the shift personnel warned that the specified rate must be adhered to. A small amount of overheating should be considered a near-miss.

Transferring material to a tank should be a fixed amount such that the Normal Fill Level is not exceeded. Reliance on the Level Alarm High (LAH) to cut off a transfer is not acceptable. I have experience of three cases where this was used and the tank overflowed because the alarm did not cut off the transfer. How many times the pump trip switch had been relied upon and operated to stop the transfer I do not know but I suspect many times. Monitoring the operations could identify this case as exceeding the SOP and stopped before an accident actually happened.

Monitoring the work of process operators and analysis of the data identifies the operational irregularities which could foreshadow accidents. A full knowledge of the risk level occurring in the operations ensures that the management is in full control of the process. It provides active safety indicators of all the hazards identified for the whole plant.

MONITORING THE OPERATION OF EQUIPMENT

Monitoring the condition of some equipment is carried out by detailed crack inspection but crack identification could be continuously monitored and then analysed by comparing the data with the limits set in the appropriate standards. Other areas which should be monitored are for example:-

- Compressor vibration,
- Operations out of sequence,
- Abnormal pump pressures,
- Reaction temperatures profiles out of normal pattern,
- Relief valves lifting below their set pressures,
- Alarms left isolated,
- Surge pressures in pipework.

MONITORING THE OPERATION OF THE PROCESS

With computer controlled plants many critical factors are monitored continuously and variation from the normal SOP is immediately high lighted by an alarm so that the process can be brought back in line. The frequency of some of these events could be part of the process data to be established and considered whether any alterations are necessary. Some aspects of the process could, with advantage, be monitoured and the data compared with the limits set in the SOP for example,

- Reactor temperature variation
- Reactor pressure variation
- Variations in impurities
- Quality and energy efficiency of the process

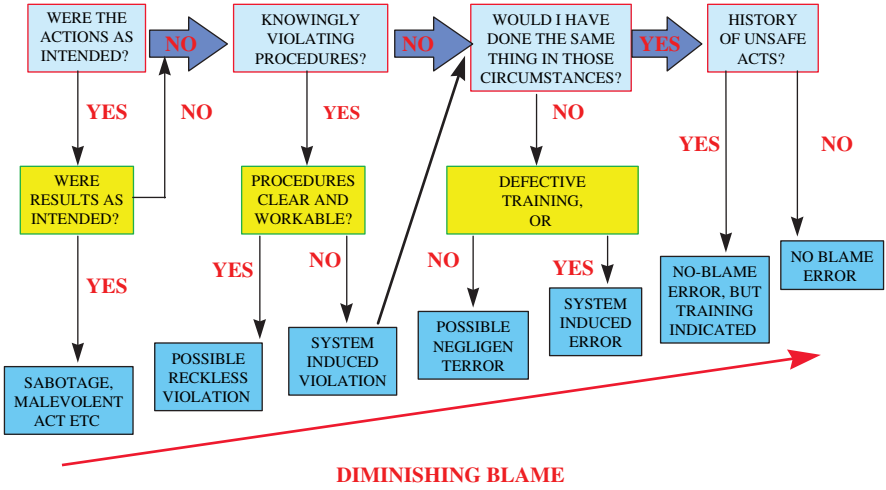

Figure 4. Disciplinary action

THE IMPORTANCE OF A JUST CULTURE

If the process staff are to be monitored it is imperative that the concept of the Just Culture system is adopted throughout the company as without it there will be no reporting of incident information and the monitoring system will quickly break down. Figure 4 shows the logic of the system adopted by one UK company.

The CAA recognises the Just Culture approach and encourages companies to take the disciplinary action. The CAA has stated (ALCOTT 2006):

> *"We promote a just culture. Since 1976 the CAA has run a mandatory Occurrence Reporting Scheme where we have asked industry to submit to us the quite low level incidents that are happening in the industry. We have given a guarantee that we shall not take punitive action against those people who report to us, except in cases of gross negligence. We expect industry to behave in the same way and to use that data with us for continuous improvement ……. We can then work towards the 'let us not let this happen again' type of scenario."*

SHARING INFORMATION

Hazards can be recognised not only from the operations carried out by the operators but also by managers recognising the advantages of sharing lessons learnt from accidents. The Responsible Care Programme, the COMAH Regulations, the recommendations of the Texaco Refinery Fire of 1994 and the recent Buncefield Standards Task Group Final Report

all require sharing of lessons learnt from accidents. All staff must be treated equally and therefore managers must also be monitored. The sharing has to be in the whole industry, not just the organisation.

REGULATORY AND INVESTIGATION BODIES

In the aviation industry accident investigations are carried out by the Air Accident Investigation Branch (AAIB) who is independent of the CAA regulatory body. The AAIB has the right of entry to investigate accidents involving aircraft. In the Regulations (AAIB 1996) they have an objective:

> *"The sole objective of the investigation of an accident or incident under these Regulations shall be the prevention of accidents and incidents. It shall not be the purpose of such an investigation to apportion blame or liability. The provider of any evidence given to the AAIB cannot be used in other court actions. This ensures that the full evidence can be given to the investigators. The results of the investigation and all recommendations are made available to the public."*

A similar situation exists with the other transport industries in the UK and with the Chemical Safety and Hazards Investigation Board in the USA.

CONCLUSIONS

The Health and Safety Executive (HSE) has a duty of investigating accidents as well as being the regulatory body. It might be thought advisable that these two duties be separated, as in the aviation, rail, marine industries and some European regulatory bodies. This would allow the investigation to be carried out to establish all the causes of the accident rather than to find a person to blame. This would leave the disciplinary side to consider whether a violation of a regulation had been established. Because a company with a Just Culture approach would take disciplinary action against its employee as necessary the HSE could then be relieved of much of its work.

The monitoring system of people, plant and process allows the critical operating parameters for all sections of a process to be under the control of the management. They will have knowledge of the level of risk of each identified hazard and any variation will be quickly identified and can be readily rectified.

This approach of an evolutionary management system should meet the requirements of the Baker Report to "… implement an integrated and comprehensive process safety management system that systematically and continuously identifies, reduces, and manages process safety risks …"

If hindsight is defined as wisdom after the event, learning the level of risks by the monitoring operation and analysing the cause of the errors becomes an evolutionary process of converting hindsight into foresight. Any modification to the operation in order to improve safety can then be readily monitored and an evolutionary management system is thus developed.

REFERENCES

AAIB 1996 The Civil Aviation (Investigation of Air Accidents and Incidents) Regulations 1996 Statutory Instruments 1996 No. 2798.

Alcott 2006 "The Economics and Morality of Safety – The Civil Aviation Industry". B. Alcott, Royal Academy of Engineering, ISBN 1-903496-26-8. April 2006.

Baker 2007 "*The Report of the BP US Refineries Independent Review Panel*" The Baker Panel Report 2007. www.safetyreviewpanel.com

Bond.1975 "The Two Safeguard Approach for Minimising Human Failure Injuries." J. Bond, The Chemical Engineer, April, 1975.

Broers 2005 "*Risk and Responsibility*" Lord Broers BBC Reith Lecture 2005.

CAA 2002 "Final Report on the Helicopter Operating Monitoring Programme (HOMP) Trial" CAA Paper 2002/02.

CAA 2003 "Flight Data Monitoring" Civil Aviation Authority, Safety Regulation Group CAP 739 2003 ISBN 0 86039 930 3 www.caa.co.uk

Global 2004 "A Road Map to a Just Culture: Enhancing the Safety Environment" Global Aviation Information Network First Edition September 2004.

HSE 2007 "Safety and environmental standards for fuel storage sites" Bruncefield Standards Task Group Final Report 2007.

ICAO 2006 "ICAO Safety Management Manual" International Civil Aviation Organisation Doc. 9859 AN/460 First Edition 2006. Available on the internet.

Reason 1998 "Achieving a safe culture: theory and practice." James Reason *Work and Stress* 1998, Vol. 3 page 293–306.

Reason 2005 "Managing the Risks of Organisational Accidents" James Reason Ashgate Publishing Ltd. 2005, ISBN 1 84014 105 0.