# THE MANAGEMENT OF RISK – AN EVOLUTIONARY SYSTEM THAT IMPROVES SAFETY

John Bond

This paper describes some of the work done in the helicopter industry to improve safety of operation. The principle involved could be adopted in the petrochemical industry to produce a similar and significant reduction in individual risk and to improve safety. Additionally there can be an improvement in quality, efficiency and reliability of operation. The important principle involves a process which is operated in such a manner that information is generated, recorded and analysed against the Standard Operating Procedure to improve safety. This ensures that the risk levels involved in the operation are continuously monitored and reduced. This evolutionary safety management system ensures that the manager takes full responsibility for the control and continued improvement in safety on the plant.

KEYWORDS: risk; risk levels; risk assessment; risk monitoring; evolutionary safety management

## INTRODUCTION

Major hazard sites in the petrochemical industry are under review as a result of the findings of the report on the incident at the Buncefield fuel depot in December 2005. Under the COMAH regulations (COMAH 1999) the management of hazardous sites are required to:

1. ensure that the risks to people either employed or who are adjacent to the site are as low as reasonably practical (ALARP),
2. prepare emergency plans and inform those in the area around the site,
3. give information to the local authority,
4. give the HSE a safety report which shows the control measures adopted,

The first requirement above involves the individual and the societal risks; the latter however is also dependent upon the population around the site, weather conditions and other factors. The second and third requirements are reasonably straight forward. The fourth requirement is very much concerned with the control of operations by the manager.

The regulatory authorities of many countries have concentrated a lot of effort on societal risk but they have found a large difference in frequencies in the catastrophic failure of vessels. Nussey (NUSSEY 2006) found:

> "*The PB99* (Netherlands Purple Book) *default failure frequencies for the two most hazardous events are 4 to 10 times lower than the HSE values*"

A societal risk originates from an individual risk on the plant which in turn requires a number of initiating events to occur at the same time. The initiating events will vary between companies due to varying safety cultures and consequently the individual risks can vary.

The manager of a process unit, to comply with the fourth requirement, has to ensure that the measures he takes to control the individual risk levels are as low as reasonably practical (ALARP). The manager therefore must have the knowledge of the risk levels used at the design stage and subsequently monitor them by leading safety performance indicators. This system of management is not proactive as it does not cover all risks identified at the design stage. To be fully in control of the risks the manager must be involved in the monitoring of the initiating events for these risks, analysing them against the Safe Operating Procedure (SOP) established at the design stage and establishing the actual risk levels. If a reduction in the risk level is necessary or can be readily carried out, action should be taken and again monitored to ensure that the expected improvement is established. This system of evolving improvements in the risk level of the process is at the heart of the aviation industry's successful development and can be applied to many petrochemical plants.

## MANAGEMENT OF RISK

Risk assessment is a requirement under various regulations and is an important part of the management of safety. The hazards associated with the plant and process, as well as the knowledge of the initiating events, will have been assessed at the design stage using various techniques including HAZOP to give an overall assessment of the risks involved. Additionally it has to be recognised that the risk data used at design stage is not always transparent and reliable, which leads to doubts during the operation of a process. The risk assessment however will have been established to ensure that the risk levels are as low as reasonably practical. Once the license for operating the plant is approved a check is seldom carried out to ensure that the frequencies or probabilities used at the design stage are acceptable and maintained. The essence of good safety management is to identify when an initiating event for a risk becomes imminent, at which point he must take immediate action.

Pasman (PASMAN 2008) in looking at the risk data states:

> "*A typical industrial process is a complex and dynamic system for which the safety level of the system (or plant) varies with time and therefore should be monitored and the estimated system reliability continually updated.*"

Pasman gives an overview of the problems of determining the risk level in process plants. He believes that the effort required establishing the quantified risk level is considerable and often requires consultants who give varying results. Regulatory authorities often require quantified risk assessment but this data can be hidden in software and not transparent or verifiable. He states that:

> "*. . .dispersion results differ two orders of magnitude among the models used, the calculated risk values varied over five orders of magnitude at 1000 m distance to the risk source*"

In particular from the beginning of risk analysis there was uncertainty in failure frequencies of pipes, tanks, valves, etc. due to the spread of results, the scenario choice, the analyst's judgment, the quality of the maintenance and data sources all differing.

To obtain reliable results there has to be knowledge of many factors which can only be obtained by risk levels established in similar equipment of a known source and in similar companies with similar safety cultures.

## MANAGEMENT OF RISK IN THE AVIATION INDUSTRY

The aviation industry in the UK has adopted a safety management system for Western built civil airliners comprising three major points (BOND 2007)

- A Just Culture approach
- Sharing accident and incident information
- A Flight Data Monitoring (FDM) system using a Flight Data Recorder (FDR) and covering crew operations, equipment performance and weather conditions. This data is then analysed, compared with Standard (safe) Operating Procedures (SOP) and the actual level of risk established.

This has resulted in a remarkable improvement in flight safety over a period of time. Based on insurance company and Civil Aviation Authority (CAA) data for Fixed Wing Losses as a percent of Total Turbine Fleet (CAA 2002), the improvement is clearly seen. (Note: the improvements in aviation safety over the period shown can be attributed to a wide range of safety initiatives but FDM with FDR has been singled out as a most important element.)

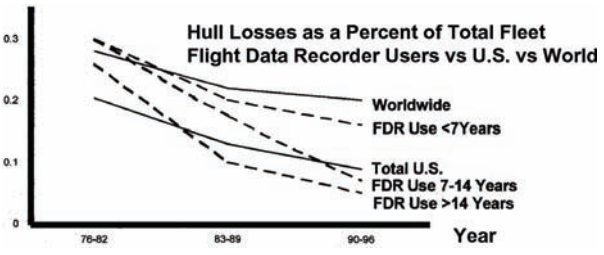


**Figure 1.** Safety benefits of FDM with FDR

The success of this approach to management of safety risks, in commercial fixed wing aviation resulted in a FDM research programme (CAA 2002) being trialled with a helicopter operator. Flight Data Monitoring is defined (CAA 2002) as

> "*. . . a systematic method of assessing, analysing and acting upon information obtained from digital flight data records of routine flight operations to improve safety.*"

The helicopter FDM programme, known as a Helicopter Operational Monitoring Programme (HOMP), was focused on monitoring the flight operational aspects of North Sea oil support operations and achieved excellent results with significant safety issues identified and action taken to correct them. The technical monitoring of such operations already existed in the form of a Health & Usage Monitoring System (HUMS) which runs parallel to the FDM system. A closed loop process was operated such that the identified risk event was monitored, analysed and an estimate of the severity level applied. Action was then taken to reduce the risk to an acceptable level. Significant improvements in the operational reliability, quality of service, economy and environmental conditions were obtained in addition to safety improvements.

Figure 2 shows the system in operation:

Data from the operation of each flight was recorded on a Quick Access Recorder and then downloaded to a computer at base for analysis. The Helicopter Operations Monitoring Programme (HOMP) software then produced four types of output.

1. Flight Data Traces (FDT) which detects pre-defined events or exceedences of operational limits and displays the flight data in the form of data traces.
2. Flight Data Events (FDE) takes the information from FDT and analyses the trends and obtains the frequency of occurrences. An estimate of the event severity is applied to each risk event as not all events carry an equal level of risk.
3. Flight Data Measurements (FDM) receives data for every flight from FDT rather than just the extreme shown in the events. By using measurements from every flight the operator can better understand normal operations of the helicopter even before events are triggered.
4. Flight Data Simulation presents an animated display of the helicopters flight instrumentation that is invaluable in debriefing of the crews and assessment of each event.

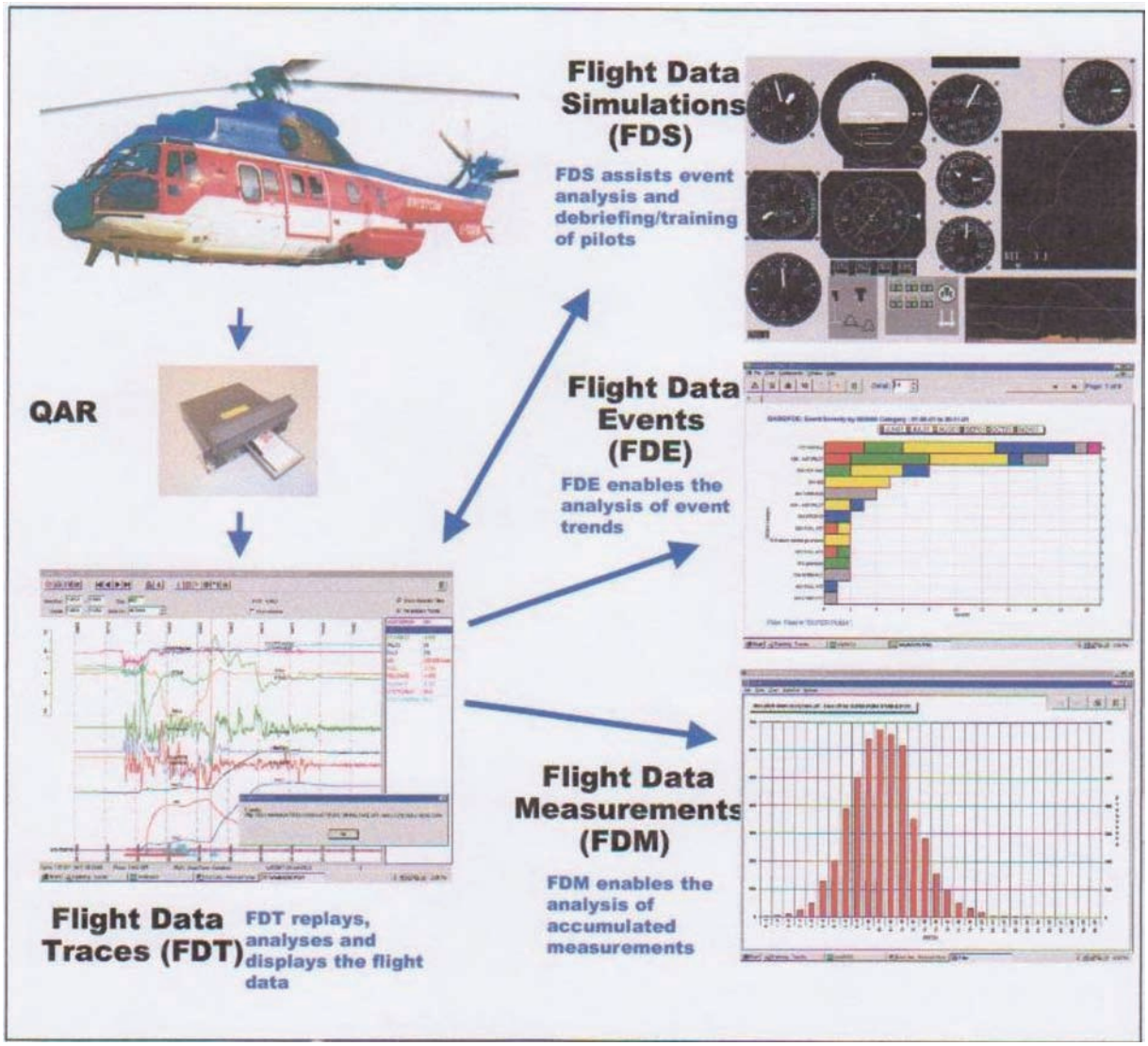


**Figure 2.** Helicopter FDM system (HOMP)

Figure 3 shows the type of trace which is analysed to identify and understand the risk associated with the events detected.

Figure 4 shows instrument panel displays used for analysis and crew debriefing.

The following was the severity guide used for establishing the risk levels of identified events:

| SEVERITY | SIGNIFICANCE OF EVENT |
|---|---|
| 0 | No significance |
| 1 | Contrary to operational standards |
| 2 | Slight risk of problem if combined with several other factors |
| 3 | Risk of problem if combined with other factors |
| 4 | Slight risk of problem as a stand alone event |
| 5 | Significant risk of problem as a stand alone event |
| 6 | Serious risk of of incident |
| 7 | Minor incident occurred |
| 8 | Moderate incident occurred |
| 9 | Major incident occurred |
| 10 | Accident occurred |

Results obtained on events show that the event with the greatest cumulative severity was 38B "Taxiing limit (right gear lifts)" which indicates there is the potential for the helicopter to roll over whilst taxing.

Figure 5 also shows other events which the manager has to address to reduce the risks of operation as appropriate. Knowing the cumulative risk event data, he is able to focus his efforts more effectively.

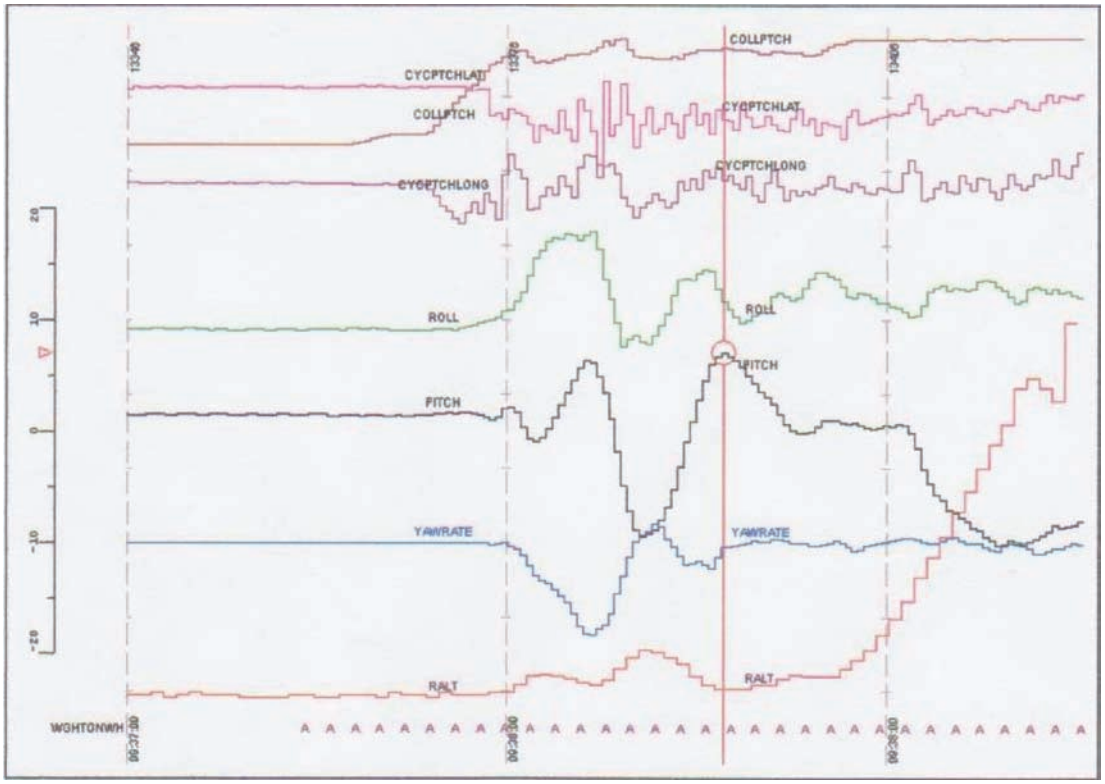


**Figure 3.** Display of flight data


**Figure 4.** Instrument panel simulations

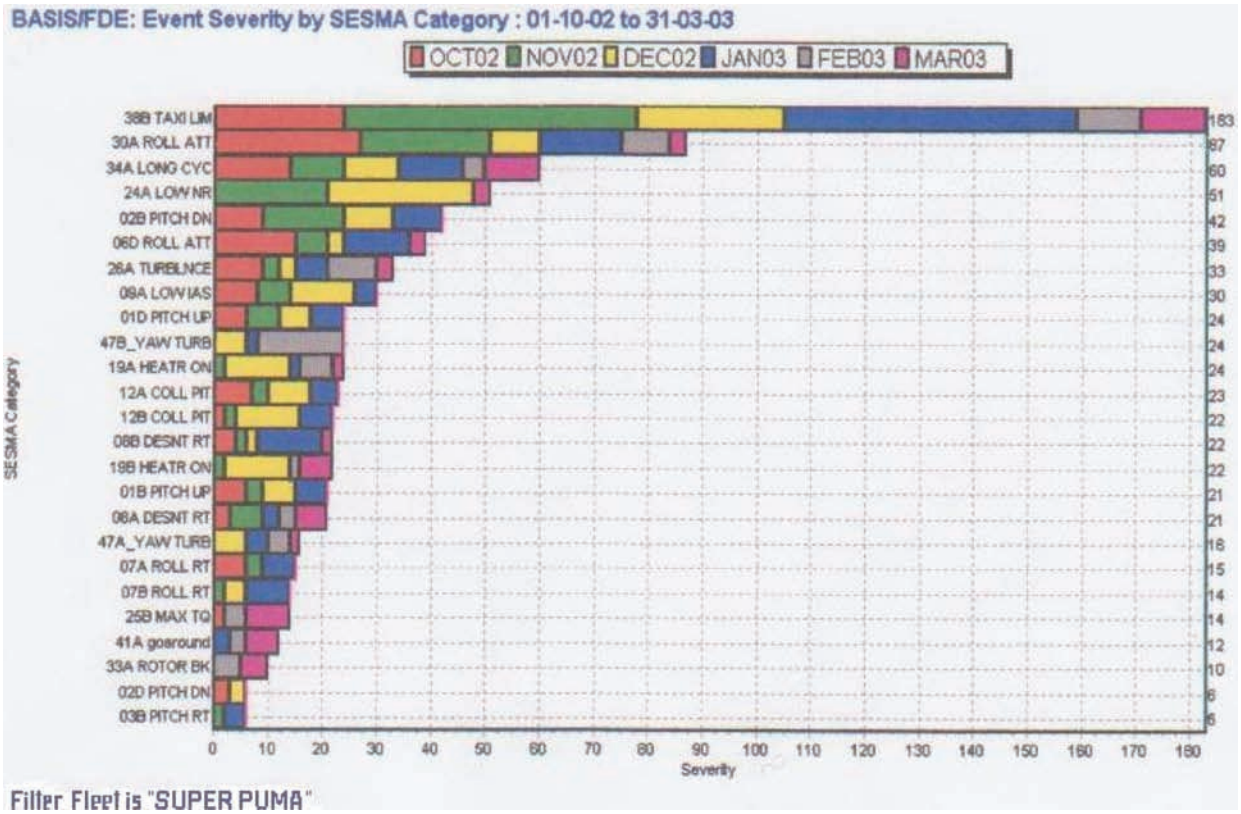


**Figure 5.** Cumulative event severity

Figure 6 shows that over the six months of the research programme the level of the risks identified were reduced significantly. Two companies then implemented the HOMP system and found acceptance by the crews as a result of the efforts made to protect the crew confidentiality and ensure that HOMP data was not misused or the results used for punitive purposes. With the event vs severity data shown in Figure 7 below (only part of the whole) the manager was made aware of his priorities for action.

The HOMP system was found to be an effective proactive system which ensured that the hazards of the

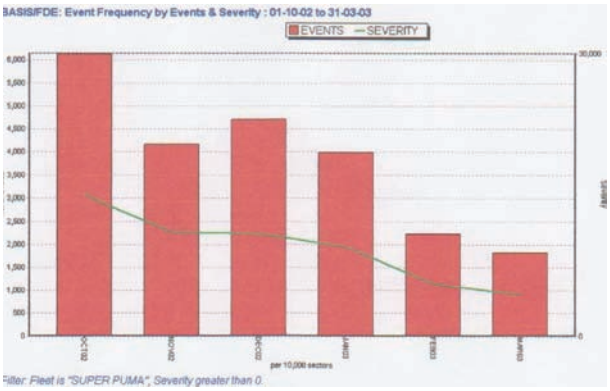


**Figure 6.** Trend of events with a positive severity value

operation were identified and corrected to make the Safety Management System an effective culture. Although the HOMP programme was applied to pilot flight operations this builds upon the previous successful programme (CAA 2006, 2008 and others) to monitor and analyse the vibration conditions in the rotors and gear trains. Known as Health & Usage Monitoring Systems (HUMS) this has proved to have been very successful in identifying developing problems prior to failure. The HOMP programme is continuing to successfully identify the risk levels in crew operation, equipment performance, helipad and weather conditions. Because of this the programme has been recommended to the International Civil Aviation Organisation for international adoption.

## APPLICATION TO THE PETROCHEMICAL INDUSTRY

Most of the initiating events for accidents in the petrochemical industry are identified at the design and HAZOP stages, and other appropriate studies. Control measures are then introduced appropriate to the risk involved. For example the control measures introduced to prevent over flowing of a tank could well be:

- Operators to be selected by approved method for responsible job.
- Operators to be trained and recorded competent in actual job.

| Event number | Title: | SF= 0 | SF= 1 | SF= 2 | SF= 3 | SF= 4 | SF= 5 |
|---|---|---|---|---|---|---|---|
| 01B | High Pitch-Up Attitude Above 20 ft and Below 500 ft AGL | 5 | - | - | 7 | - | - |
| 01D | High Pitch-Up Attitude Below 90 knots IAS | 4 | - | - | 9 | - | - |
| 01E | High Pitch-Up Attitude Above 90 knots IAS | - | - | 4 | - | - | - |
| 02B | High Pitch-Down Attitude Above 20 ft and Below 500 ft AGL | 8 | - | - | 17 | - | - |
| 02D | High Pitch-Down Attitude Below 90 knots IAS | 23 | - | - | 5 | - | - |
| 03B | High Pitch Rate Above 500 ft AGL | 6 | - | 6 | - | - | - |
| 06D | Roll Attitude Above 40 deg Above 300 ft AGL | 10 | - | - | 14 | - | - |
| 07A | High Roll Rate Below 500 ft AGL | - | - | - | 7 | - | - |
| 07B | High Roll Rate Above 500 ft AGL | 9 | - | 9 | - | - | - |
| 08A | High Rate of Descent Below 500 ft AGL | 8 | - | - | 10 | - | - |
| 08B | High Rate of Descent Above 500 ft AGL | 3 | - | 19 | - | - | - |

**Figure 7.** Numbers of events by type and severity

- Standard Operating Procedure written with transfer pump to be stopped at Normal Full Level (NFL).
- Transfer to tank to be checked that transfer has been stopped at the NFL by reading the level gauge.
- Transfer details to be entered in log.
- High reliability High Level Alarm with pump cut off.
- Testing and maintenance of alarm system at specified times.

In some cases a High High Level Alarm is fitted usually because of acceptance that the HLA is used to cut out transfer. An accident occurs if all seven safeguards break down and become the initiating events. It should be recognised that if one or more safeguard breaks down it should be considered a near-miss. In all honesty frequently some two or three initiating events are often ignored or, due to circumstances, are bypassed.

An analysis (ICHEME 2008) of the failure mechanisms in 100 incidents in oil refinery distillation units showed:

| FAILURE MECHANISMS | FREQUENCY% |
|---|---|
| Corrosion | 18 |
| Excessive vibration | 5 |
| Human error | 33 |
| Hydraulic surge/water hammer | 3 |
| Piping joint failure | 5 |
| Over pressure | 10 |
| Over temperature | 10 |
| Pyrophoric ignition | 5 |
| Pump seal failure | 5 |
| Valve failed to seat | 3 |
| Water freezing | 3 |

Taking the first failure mechanism or risk, corrosion, a list of the initiating events can be written:

| Risk | Initiating events |
|---|---|
| Corrosion at top of crude oil distillation unit. | Water separation at crude oil tank not carried out |
| | Wash water flow to desalter insufficient |
| | Monitoring pH of overhead water collection system insufficient |
| | Wash water to overhead system not adequate |
| | Draining water from reflux drum inadequate |
| | Inspection of unit to detect corrosion inadequate |

During the operating mode of the plant the initiating events were only found after an incident and after an investigation when action could be taken to implement the

recommendations. How much better it would be if one of the initiating events could be identified before the accident happened. In the Swiss Cheese model for accident causes all holes have to line up for the accident to happen. If just one slice of the Swiss Cheese (an initiating event) has lined up and can be identified and then changed the risk of the accident will have been reduced before the accident occurs. All of the above initiating events could be monitored on a continuing basis by appropriate instrumentation. They could be recorded and analysed against the Standard Operating Procedure, and a print-out would indicate whether the requirements of the SOP had been appropriately complied with.

Let us consider the 33% of accidents involving human error and look at just a few.

| Incident | Some of the possible initiating events | Monitoring events and analysis |
|---|---|---|
| Over flowing of tanks | Leaving HLA to stop pump transfer. Not stopping transfer at Normal Full Level | Record frequency of HLA activation |
| Valve in wrong position at start up | Inattention | At start up record vale position from indicator |
| Slow pressure increase leading to high pressure alarm in flare line at start up. | Blockage in sample points. Line not fully checked. | Pressure increase to be monitored and rate alarmed. |
| Tube failure in furnace. | High rate of temperature rise at furnace start up | Rate of rise to be monitored |
| Loading road tanker of ethyl acetate and ignition. | Flow rate of loading tanker too high resulting in static ignition | Flow rates alarmed for various products |

At present these incidents are only reported after they have occurred and when the event has been investigated. How much better it would be if these initiating events were identified before the incident occurred. Take the case of overflowing of a tank. This risk event occurs because the transfer to the tank was not stopped at the Normal Full Level and the operator left the pump to be cut-out at the High Level Alarm. The HLA was intended as an alarm condition to remind the operator that the level was still rising. If the cut out of the transfer pump does not occur the tank overflows. Very often a HHLA is added to ensure that the level is not still rising. If however the operating system is monitored and analysed the first occasion when the HLA operates will be recorded and action can be taken to instruct the operators that transfer has to be stopped at the Normal Full Level. If this action is not taken then it becomes common practice always to leave it to the HLA to cut out the transfer. This then means that the solenoid associated with the HLA is asked to operate far too often and will fail sooner.

Venting and draining of lines at the start up of any process unit must be carried out with care. Rust and solid particles will collect at sample points blocking the points and thus indicating that the line is clear. The solids will also collect in valves preventing their complete closure. The positioning of valve indicators and line pressure build up will indicate these problems before serious levels occur. Monitoring them becomes an important part of the start up.

Computer controlled refineries, tank farms and plant very often record the time of alarms sounding. All of this data can be analysed by software similar to SESMA (BOND 2007) used in fixed wing civil aviation, and any exceedence of the Standard Operating Procedure noted for the manager to take action. How nice it would be to see a table as follows but with numbers in the Severity Factor columns. All of the risks involved would become Leading Safety Performance Indicators

Over a period of time a table similar to that obtained with the HOMP programme would be obtained to show where the high risk events were occurring. This is shown below:

| Event number | Failure event | SF = 0 | SF = 1 | SF = 2 | SF = 3 | SF = 4 | SF = 5 |
|---|---|---|---|---|---|---|---|
| | Leaving HLA to stop pump transfer. | | | | | | X |
| | Not stopping transfer at Normal Full Level | | | | X | | |
| | Inattention | | | | | | X |
| | Blockage in sample points. Line not fully checked | | | | X | | |
| | High rate of temperature rise at furnace start up | | | | | X | |
| | Flow rate of loading tanker too high resulting in static ignition | | | | | | X |

It is very important for the chemical industry to adopt some of these latest systems in view of the aging of some of the equipment and the requirements of the Regulatory Authorities for quantified risk assessment.

## ADVANTAGES FOR THE PETROCHEMICAL INDUSTRY

The great advantage for the petrochemical industry is that having identified the risks at the HAZOP stage they can be monitored by the computer used in the operation of the plant. The analysis of the operation against the SOP may require new software. The monitoring and analysis of the risks cover human factors of operations, the equipment involved and the processing conditions. If the risks are not acceptable they can be modified and checked. This ensures that the manager is in control of all risk factors and not just a few leading safety performance indicators. Additionally the system can be applied to environmental conditions, quality issues and special systems for monitoring corrosion and vibration problems in turbines. The system becomes proactive, evolutionary and leads to a safer operation.

In addition once the risk levels are actually established ideas will flow on how to make further improvements in many areas. A further advantage is that knowing the actual level of risks in operation and under known conditions the design of new plant will be improved.

The knowledge of the actual risks by the manager of the plant will ensure that he takes responsibility for the operation and for making improvements in safety. Any expenditure that he wishes to make will be backed by actual data on the operations.

## CONCLUSIONS

Pasman (PASMAN 2008) comments that:

> "*The essence of process safety is to be aware of hazards, to estimate the risks, to reduce risks where possible, to pick up the signals when danger becomes imminent, and to know what to do to neutralize the threat. Where there is a risk, a situation lacks safety. Thinking risk will therefore result in thinking safety, although everything has its limits.*"

Adopting the principles demonstrated in the civil aviation and helicopter industries of identifying the initiating events of incidents involved in an operation by monitoring them, analysing the risks against the SOP and taking action to rectify any exceedence will result in improvements in safety. All of this can be done by computer to give the data the manager requires to exercise his responsibilities in the safe and effective control of the operation of his plant.

This evolutionary safety management system is a way forward for improvements in safety as well as satisfying the growing demands required by the public. 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.*"

The aviation system meets this requirement very fully and has shown it to be effective in risk reduction.

## ACKNOWLEDGEMENT

The author wishes to acknowledge the help of David Wright of the Civil Aviation Authority in the provision of information and figures used in this paper and for permission to use some of their graphics.

## REFERENCES

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

BOND 2007, "Continuous Monitoring of Risks – People, Plant and Process" Hazards XX IChemE Symposium Series No. 154, 2007.

COMAH 1999, The Control of Major Accidents Hazards Regulations 1999.

CAA 2002, "Final Report on the Helicopter Operations Monitoring Programme (HOMP) Trial" www.caa.co.uk

CAA 2006, CAP 753 Helicopter Vibration Health Monitoring (VHM) Guidance Material for Operators Utilising VHM in Rotor and Rotor Drive Systems of Helicopters. June 2006 www.caa.co.uk

CAA 2008, CAA Paper 2008/05 HUMS Extension to Rotor Health Monitoring. December 2008. www.caa.co.uk

ICHEME 2008, "Hazards of Oil Refining Distillation Units", BP Process Safety Series, IChemE, 2008, ISBN 978 0 85295 522 2.

Pasman 2008, "Risk Analysis: History, Problems, Perspective!" www.hipasman@gmail.com