Human Error: Anatomy of Accidents

Anthony J Spurgin
Independent Consultant, San Diego, California, USA

Abstract: The paper examines various industrial accidents and lists the lessons that can be learned from their study. These insights can be used in a number of ways, such as improving an understanding of the causes of human errors and impact the modeling of human errors, selection of human reliability assessment methods and models. Accident analysis can also be used to identify how the structure of Probabilistic Risk Assessments (PRAs) could be improved by incorporating ideas derived from these investigations.

Keywords: PRA, Human Errors, HRA Methods, Accident Analysis.

1. INTRODUCTION

The purpose of this paper is to review a number of industrial accidents in some detail and derive some lessons from these accidents that might influence analysts' selection of HRA models and methods to be used in their PRA studies. The study of accidents can help the HRA community realize that HRA is not just selection of a human error probability (HEP) number to place into a systems logic that supposedly represents an operating plant. The PRA should represent the way that the plant is designed, constructed and operated at all levels, from management, operations, training department, and maintenance services. The accidents covered below cover a number of different industrial areas from nuclear plants, aircraft operations, chemical and oil/gas operations and railways.

The role that humans play in any accident can vary. In some cases, the design selection of equipment can play an important part, in other cases the decision of management can affect the accident progression and other cases the training of operation staff can be the key element to terminate or mitigate the accident or aid in making the accident worse. Most of the accidents considered here have been reported in both the technical press and news papers and are mostly well known.

2. ACCIDENTS

Table 1 shows a number of accidents that have occurred in various industries from Aerospace to the Chemical Industry to Railways. A couple of the accidents have been selected for a more detailed discussion. In discussing any accident, one needs access to good reports relating to the details of the accident. This is not always possible. The national/international media usually provides the first report of an accident, but often details are missing. Later, often much later there is an official report produced by governmental agencies, such as the US National Transport Safety Board (NTSB). Some countries call for a formalized enquiry such the United Kingdom. In the case of the UK, the government calls for an enquiry headed by an eminent judge of the high court, this was the case the Piper-Alpha accident headed by Lord Cullen [1.]. In the case of the NASA Challenger shuttle accident, a high level Commission was formed under the leadership of Mr. Rogers [2.] to produce a report with recommendations for President. The quality of the accident report depends very much on the efforts made to discover the causes of the accident. However, often from the point of view of the HRA expert, the insights are often lacking details related to human performance.

Accident analysis processes seem to be very much related to coming down to a number of possible causes and reporting these to the public in some official manner to show that the governments are responding to the situation. The results of the study are then released and the owner of the facility is fined and says that the problem will be 'engineered away.' This may be a cynical view of the response. However, the HRA specialist would like to look deeper at the causes of an accident to see

what are the deep causes? Particularly we are interested how the humans modify the accident progression and how their actions are affected by the situation. Often accident analysts complete their reports with the words; 'the accident was due to human error'! From the HRA expert's point of view this is not sufficient. It is believed by many HRA experts that the context under which the humans function play a strong part in the accident progression and therefore one needs to understand how the operator(s) were affected and ended up in an accident. It should be noted that very few persons, such as pilots, are interested in committing suicide and killing others. Yes, people do make mistakes, but the author's feeling is that a large numbers of times the circumstances of the accident and the associated context play the major role in determining if humans act erroneously. If we understand these circumstances or contexts then in the future, the potential accident rate could be reduced and recovery rates enhanced.

Table 1: List of Accidents

Industry	Accident	Consequence
Nuclear	3Mile Island 3/79	$2 Billion, no deaths short term
Nuclear	Chernobyl 4/86	Deaths:36 short 4000 long term +++
Space	Challenger 1/86	Shuttle loss and crew(7)
Space	Columbia 2/04	Orbiter and crew on re-entry
Air Transport	Tenerife 3/77	2 x747s crews and most passengers (583)
Air Transport	JFK 11/02	Airbus 300, 265 plus 5 on ground
Chemical	Bhopal 12/84	3,000 plus at least 8,000 deaths that occurred later
Petro-Chemical	Texas City 3/05	$1.5Billion, 31 deaths, 100injured
Oil-Rig	Piper Alpha 7/88	$3.5 Billion, 165 deaths
Rail Way	Flaujac 8/85	31 deaths & 91 injured
Rail Way	King's Cross 11/87	31 deaths

3. DISCUSSION OF SOME ACCIDENTS

It is not the idea here to discuss each accident in detail, but rather identify a number of the key characteristics of accidents. For details about the accidents, one either track down each accident report (Google or Wikipedia) or examine the coverage in Spurgin [3.]. The intent is not to show that many accidents follow the classic PRA logic, but to indicate that the totality of an assessment is more than a blind application of PRA ideas. All of the accidents have the ingredients of an initiator, human actions and the combination of equipment failures and/or their unavailability. The only question is how are these selected, what are they due to and how do they come about? The consequences of the accident can vary depending on the actions taken in response to the accident. Some actions are the result of instant activities undertaken by the operating personnel to terminate or mitigate the effects of the

accident and others are taken ahead of time, such as the design and installation of automated spray systems and, as in the case of some nuclear power plants, the physical containment, to prevent radioactive contamination of the surrounding area and leading to the death of persons.

3.0. Introduction

By looking at accidents, we see that the availability of equipment and its design characteristics are due the selection processes made during the design phase and rests with the manufacturer and agree to by plant management. The preparation of the operational staff rests with the management, including the use of the appropriate procedures, and the development of the operators' knowledge and skills. The general vigilance of the staff is a product of the attitude of management. The interface between the machine (power plant) and the operational staff is a combination of design (Human Factors) and industry norms. In fact, the industry as a whole enters into consideration as a 'cultural impact'; 'we do things like this here, not like they do in Xland'.

This suggest that in performing a PRA, we need to be aware of not only that there are persons performing given jobs; such as the main control-room crew, the maintenance and test personnel, the supervisors and plant management, but also how the plant has been designed, operated, maintained and tested. It could be that because of the role of regulation (NRC) and industry supervision (INPO), and the safety culture of the NPPs; the task of the PRA analyst is eased and one can follow same rote process in assessing the risk of NPPs. By virtue of the need for the regulators and the industry supervision and the fact that they report problems, one realizes that all is not as uncomplicated as it seems. So does the PRA really capture the nuances of variations in plant safety inherent in the whole process, such as the variations in the design of the plant, and management styles?

Reviews of accidents in various industries indicate both complexities and variations in the balance of the various contributions. Some of the key elements in accidents are indicated below. These indicators are the author's responsibility and not necessarily ones that others might agree to, but it does show something of the distribution of contributors. It also indicates the key role of management in the causality of accidents. Of course, which does become clear is that sometimes decisions are made by the design group early in a project that affects later operations, so the current management cannot held to be responsible for those decisions! The author suggests, that by these examples, by defining an accident as being due just to human error is naïve, the human maybe the last element in set of dependant parts and his action could predicted based upon the context of the accident. Society's view of humans and their capability can vary from thinking them as supermen or incompetent persons. A trained person has a number of features that are defined by circumstances under which he operates and his probability of success or failure depends on the organization understanding those conditions and modifying them to enhance the probability of success.

3.1. Accident Features

For each accident listed in Table 1, the key influences that affect the accident progression are identified below. This is the author's list and again others may have different opinions.

1. **TMI #2 NPP**: The selection of once-through steam generators with low water storage capacity (design), Poor Training of operators in reactor dynamics (Training) and inadequate post maintenance checking (Management).
2. **Chernobyl NPP**: Failure to solve issue with diesel reliability (Design), poor risk assessment of test (Management) and poor training of standby staff (Management and Training).
3. **Challenger, Space Vehicle**: Booster rockets were vulnerable to low temperature ("O" rings) and to vibration (longitudinal flexing) (Design) and given these problems the decision to launch under cold conditions was incorrect (Management) given prudent engineering advice.
4. **Columbia, Space Vehicle**: Inadequate insulation of large fuel tank (Design) lead to insulation breaking off and damaging carbon insulation of the Orbiter vehicle wings needed for re-entry. Indications were available from past operations that chunks of insulation could detach and hit

the carbon heat insulation, which is fragile. Failure to redesign insulation of the fuel tank and provide an escape path for the crew to enable successful re-entry (Management) .

5. **Air Transport-Tenerife**: Selection of a poor overloaded emergency site with runway problems (Aviation authority), poor local control of the runway access and inadequate communications (Local Management). Failure of Pan Am aircrew (Human error) to follow instructions, but could have been aided by local staff monitoring aircraft movements. Failure of KLM pilots (Human error) to be more cautious given poor quality of communications.
6. **Air Transport- JFK**: Ground controllers and flight organizers allowing Boeing 747 and the lighter Airbus 300 to take off in tight order (Airport Operations Management). Over-reaction by Airbus 300 pilot to oscillations caused by 747 vortices affecting the 300 (Pilot Human error). Pilot responses were partially induced by wrong training (Training) for a 'light' 300 tail assembly that seems too fragile (Design). Some questions arise on the design side because of the missing plant in a flight from Brazil to France over the Atlantic.
7. **Bhopal Pesticide Plant:** Failure to design adequate means for preventing the release of large quantities of Methyl Isocyanate (MIC) (Design and Management), Failure to realize that the plant could be sabotaged (Management), Failure to prevent large numbers of the Indian public from living the exclusion zone, (Management, Bhopal and Indian Governments), Failure to provide a warning system and training for local citizens (plant management and Indian Government). Post accident reviews were not helped by Indian Government interference.
8. **BP Texas City-Oil Refinery:** Poor instrumentation and inadequate alarms (Design), inadequate training of operators (Training), mismatch between tower and dump tank capacities (Design), trailers for plant personnel in the exclusion zone (Management) and inadequate fire suppression systems (Management). A large number of pre-cursor fields did not alert Management to future problems.
9. **Piper Alpha Oil/Gas Rig**: Rig designed for oil exploration, but was used for gas exploration; the design was unsafe for gas explosions, wrong use of design without changes. Fires lead to explosions (Design, Management). Crew protection was poor and unsatisfactory (Design and Management). Coordination of undersea operations limited response to fire, by the use of pumps (Management). Maintenance activities were poorly planned, notice of activities poorly registered. Operations staff used initiative to regain control to meet rig objectives (output), but failed to realize interactive effects of the actions (Maintenance, Management), issue of training and procedures. Fire made worse by failure to coordinate cut-off of flows from other rigs (Overall Management and operational design considerations [warnings at other rigs]).
10. **Railway-Flaujac, France**: Basic design fault determined by cost of track (Design), system relies on a single track with by-passes. Signaling system relies on published time charts to be interpreted by staff, rather than an engineered safety system (Basic Design Philosophy). Time schedules changed depending on the day (Human Factors/psychology). Coordination between stations and rail crews were not carefully procedurized with callbacks (Procedures). Experienced station controller replaced by inexperienced person with inadequate training (Training, Management).
11. **Railway-Kings Cross Underground station, London**: Failure to investigate reasons for past fires and a failure to consider the possibility of a large fire leading to many deaths (Tube Management, and Safety Authority). Wrong diagnosis of fire and potential problems that could occur (Local Fire chief, lack of deep understanding of fire propagation). Kings Cross did not provide well designed safety escape routes and protections for passengers (London Authority). Escalators were fitted with wooden steps, did not help the fire situation along with poor choice of paint (Design). The Tube (London Underground system) has grown over many years and like many government run organizations has probably been under-funded and things like unique safety aspects had not been fully investigated. During the Mr. Fennel QC inquiry [4.], it was discovered that in open ducts fires can progress downwards! The fuel to help start the fires was waste, oily rages, bits of paper, etc and the source was dropped lighted cigarettes! (Failure of Maintenance and Management). So truly cleanliness is close of godliness!

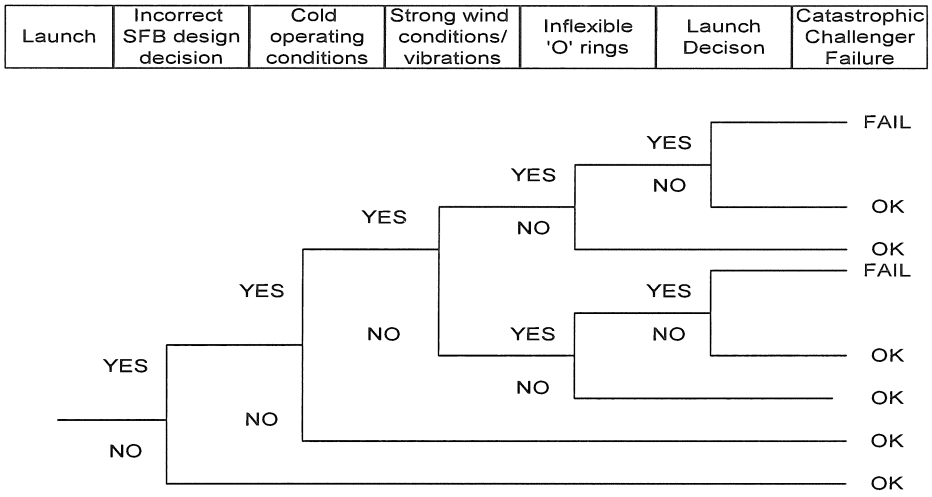
3.2. Analysis of Accidents

This section relates to the analysis of accidents based upon the approach used in PRAs to understand the event sequence of an accident during the early analysis stages of a PRA study. Event sequence diagrams (ESD) or a Decision Trees (DT) can be useful tools to look at the effect of possible events that can take place during an accident. Here the accident reports were examined for the events that actually occurred and in some cases other events that might have occurred were added. For each of the accidents event diagrams were constructed along with the identification of each end state. The advantage of using the trees is that one can quite easily see the relationship of any event on the consequence, i.e. if a particular event does not occur then the consequence of the accident is lessened or does not occur. One can also see that the idealized PRA triad-Model, yielding the highest probability, may not occur.

A couple of trees are given here to illustrate the usefulness of the tools for examining accidents and possible solutions to ensure that they do not occur in the future. The trees illustrate the utility of capturing the main elements of an accident and along with speculations about how different pathways can lead to success or failure. Some accidents have a large number of elements or headings and others have very few. Two trees shown below are for the Challenger and Bhopal accidents.

The first tree (Figure 1) covers the various decisions made by NASA that lead to the accident. It appears that some decisions were not good given the attitude of NASA management, in others words if launch management was prepared to live within the limits of the accepted design, then it was possible that the accident would not have occurred. Unfortunately, they were not prepared to defer their decision to realities of life. Given a different design, their decision could have been made and all would have been alright. The cautionary comments made by engineers were overridden. Persons reviewing the initial design did not seem to have considered how the Solid Fuel Booster Rocket structure (jointed structure with "O" rings) might be affected by temperature, winds and vibration. The structure seems to have been optimized for transportation reasons and possibly cost. The limitation of the "O" ring design was indicated by earlier bypass burns. This information was available to the decision-makers. One could argue that the design was acceptable, provided that its limitations were bourn in mind. It is pointed out that the wind and vibrations could be considered contributory effects, making a bad situation worse! Figure 1 has a number of headings each related to decisions and conditions. The yes branches correspond to decisions agreeing with the headings, for example if the "O" rings are inflexible then one takes the yes branch and so on. One can see that there are possibilities for correct launches as well poor launches, unfortunately the wrong decisions were taken and this lead to the accident.

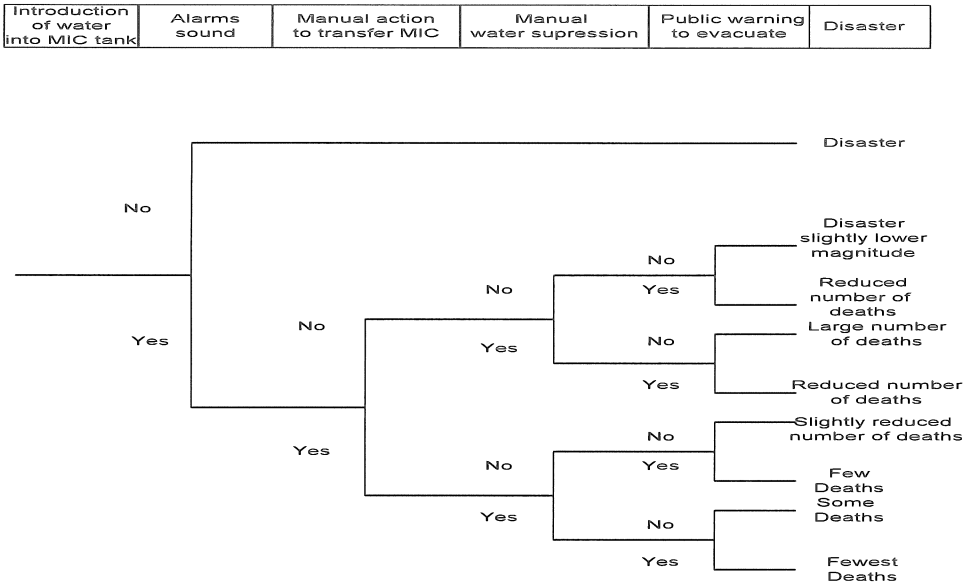
Figure 1: Decision Tree Associated with the Launch of the Challenger



One can see that there are a number of branches, the first branch relates to the SFB design being good or otherwise. The conclusion is that if there was a good design then would be alright, but really there may have been short comings in the alternative design and this is not considered here! At the core of the incorrect design were the layout of the joints and the selection of the "O" ring material. The design of the joint was such that flexing of the booster rocket could lead to opening of the "O" space. The "O" ring was expected to move to seal the gap and this occurred most of the time, but when the temperature was cold the "O" ring was less flexible and did not take up the space, leakage of hot gases occurred! In the case of the accident the hot gases impinged on the large fuel tank and it exploded leading to the loss of the Challenger. NASA's subsequent actions have been to redesign the joint with more "O" rings!

The second tree (Figure 2) is a decision tree for the Bhopal accident; see Kalelkar [5.] for details of the accident. This is possibly the worst accident to have occurred world wide, in terms of numbers of people killed and injured, beyond the decisions to go to war. The pain and agony inflicted upon the population of Bhopal was tremendous and could have been avoided with the proper safety precautions. The accident is judged to have been caused by the actions of a disgruntled employee, although other causes have been suggested, but not very believably. The tree, shown below, focuses on elements that could change the sequence to result in lower deaths; it appears that beyond preventing the ingress of water into the MIC, for any other of the actions some number of deaths would occur!

Figure 2: Event Sequence Diagram for the Bhopal Accident



It is seen that it was possible to save more people, but ultimately once the accident was underway there was nothing that could be done to save people except to get them out of the proximity of the MIC dispersion. It is thought that this was impossible; there was no means to move all these people given the shortage of time and the public transport facilities available. Once the water was placed in the MIC tank the inevitable conclusion was that a large number of people would die in a painful manner. If the management (both US and Indian) had carried out such analysis then they should have taken steps to ensure that water is not introduced into the MIC tank. If by chance this happens, then the design of the plant should ensure the relief flow is dumped into a protected vessel not into the atmosphere. The steps taken by the US nuclear designers was quite correct in having a containment to prevent the escape of radio active nuclides into the atmosphere, if there is core damage. The chemical industry should accept the concept that the public needs to protected from chemical releases and

maybe one way to do this is to have containment structures to ensure that things like MIC cannot be released so easily!

Various alternatives have been considered and lie within the plant design and operating procedures and these are indicated by the headings shown in Figure 2. The assessments of the efficacy of the mitigating functions are the author's, since this kind of data/information was not available. In fact, it is not clear that any such analysis was carried out by the plant designers. The key issues for management were how do we prevent such an accident occurring and if it does occur what do we do prevent the MIC escaping? It appears that no such thoughts were carried out. One issue associated with engineering designers is the tendency to work in success space rather than failure space. Our designs are going to work, based upon past experience, and therefore there is no need to consider if they do not! A compounding problem in the case of Bhopal was the fact that management was considering shutting down the plant and the staff was concerned with losing their jobs. It is know that under these conditions, sabotage can occur with the idea of prolonging employment. It is believed that this is what occurred here. The intent of the saboteur was not to take an action that could lead to so many deaths, but merely delay closure of the plant. Of course, this cannot be proven since the person responsible has not been found, so we cannot know his intent.

4. REPORTING OF ACCIDENTS

The quality of what can be learned from accidents depends on the reports generated as a result of the accident. In addition, the quality the report depends on the agency performing the review and their objective in undertaking the review. For example, the large government reviews, like the President's Commission Report on the Space Shuttle Challenger Accident [2.] and Lord Cullen's report [1.] on the Piper Alpha accident are very good in depth reports.

Other accidents are not so well treated; sometimes a report is available over the internet from the organization involved in the accident, like the Texas City, where a report on the accident was release by one of the persons from BP Broadribb [6.], who was called in to investigate. This report is good. The insights gained from the accident reports can be of direct use for the HRA expert, however the expert can perform his own analysis given these reports.

One can even learn useful information from newspapers, TV and radio (the media). The on-site reporters can glean information by their own observations and also by clever interviewing of participants. Unfortunately, the world of reporting has changed from capturing the best information and presenting that to the readers/listeners to creating (or spinning!) the news!

Some of the accidents reports have their own way of proceeding which can color the information. The NTSB seems to be satisfied with their reports up to the point of finding the error as being due to the pilot or some other cause. The Airbus accident is a case in fact. The NTSB found the pilot (pilot error) to have used the wrong technique as far as responding to disturbances coming from the 747. Maybe behind the scenes they put out another message, but the author considers that the pilot was not entirely to blame. There have been cases, where a light plane has been blown over by the wake of a 747! This was hardly, pilot error, the light plane was taxing on the runway under the control of the tower and stationary! The power of a wake is proportional to the weight of the plane, hence the reason they use the terminology 'heavy' for 747 planes!

The issue with the NTSB approach is having determined that the cause of the accident is pilot error, what do you do about it? There always going to be erroneous acts by humans! Coming up with some platitudes or non-solutions to the issue is not going to help. We need to determine as well as we can what was about the situation that lead to the accident? Once we are in a better position to understand the situation, which should enable us to design better ways of reducing the accident rate. Sometimes one has to redesign the process, for example in the case of a Los Angles' rail accident (driver text messaging), see LA Times, Rubin et al [7.] the basic fault was the design of the rail system (Metro

Link) and eventually any random driver error could lead to an accident. The driver was at fault but later some other issue would occur and there would be crash. Putting in an automated train stopping feature could lower the rate of accidents to make them somewhat more tolerable. The idea of using video observers of the driver might only work in the short term; it does not get rid of the basic problem. Solving problems by assuming the operator is highly reliable is non-sense, it is better to use more realistic and achievable assumptions and design the system in a better way.

5. LESSONS LEARNED

So what are the lessons to be learned from a review of accidents? Firstly, the role of management decisions plays an important part in both the cause of accidents and their progression. When one talks about management, this may be considering decisions made over a span of time by different managers. So plant designs fall into the province of the early management team and even made by the plant designers without the subsequent plant owners being aware of the implications behind the decisions. One can see this in the case of the shuttle design. In a way, the booster rocket design lead to a sub-optimal design of the shuttle, this limited its launch capability. During the design phase of boosters, was the question of operational limits even considered, related to the effects of weather on the functionality of the shuttle?

This brings up the point that there is a need to perform an early risk evaluation of proposed designs. Although it is not possible to address all issues, one can begin to examine the inter-relationship between design and operation. In this way, some of the short comings of the selected booster rocket design could have been identified and operational limits to the launch of the shuttle addressed. If the requirement was for complete flexibility then maybe an alternative design would have been selected.

The point of undertaking accident analysis is to try to understand as much as possible about all aspects of design limitations along with operational problems. The answers to the following are needed, how did the accident, was it due to equipment failures, organizational failures, effects of weather, etc and was it caused by humans or was it not terminated successfully, and so on? As stated above, the quality of the accident reports can help or hinder in determining what steps are needed to try to prevent such accidents occurring in the future. Some large scale investigations have focused on many aspects including the short comings of the design of the plant, of the plant management and even lack of industry standards, as contributing to the accident progression.

One area that has not received sufficient investigation has been; what are the influences that caused operators to take the actions now labelled human errors? The field of human reliability assessment has tried to predict the probability in risk assessments, but very few HRA experts have been involved in the process of assessing the causes of human errors in accident studies. The author would have thought that there should have been a much closer relationship between these two fields. Dekker [8.] has suggested that accidents cannot be properly analyzed without considering the pilot's view of things and this is what HRA should be about.

The author has tried to fill in gaps in the accident reports with respect to influences that may affect the operators' performance drawing upon his HRA experience. The performance of the operators is influenced by the environment under which they are working, i.e. the view from the pilot's seat, Dekker [8.]. The environment covers a number of things such as the quality of the training the operators receive, the quality of the information systems as they supply the

appropriate information for the operators to base their actions on, the attitude of the management to support the operators decision-making, the quality of the procedures in assisting the operators in making the best decisions to avoid, terminate or mitigate an accident. Accident reports need to address these issues as well as listing equipment failures or lumping operator actions under the global human error designator!

The lessons learned from accidents are that they are quite complex and can involve influences stemming from the design of the plant and its optimization, the role of management in conditioning plant operations, such as selection of personnel, controlling procedures and training and by their interactions in operational decision-making. It should be the role of management to take steps to improve the situation under which the operators function. The staff can suggest ideas, but it is up to management to take the necessary actions and generate the atmosphere under which ideas are really accepted that can lead to safer economically run plants.

6. PRA LIMITATIONS

The generalized structure of the PRA has not been changed much over the years from the early Safety Study, WASH 1400 [9.], so you could argue that the original team did very well. Since that time, there have been a number of improvements in techniques, modeling, common cause implications, etc. The Three Mile Island #2 accident, Kemeny [10.] raised the awareness that the contribution of the plant operators to the safety of Nuclear Power Plants (NPPs) was more important than had been envisioned in the early days of nuclear power. The impact of the contribution of humans to the safety of NPPs has grown as reflected in the importance of the human contributions in safety assessments (PRAs). For the early PRAs, the human contribution was assessed to have been about 15% and in later studies this has risen to about 60% to 80%. This increase in assessed contribution mirrors the change in focus from the automated shutdown systems required for reactor shutdown to the requirements for operator actions to ensure the removal of decay heat. The failure of the operators to carry out these actions successful, impacts the safety of the plant.

Looking at the structure of the PRA, one sees that the role of the main control room operators is very important, along with equipment failures; both dynamic and static elements play an important part in plant safety. The maintenance and testing staff can disable equipment thus reducing the redundancy of equipment and all staff can be in a position to initiate accidents. It would appear that the role of management and plant designers is considered to be vital by virtue of prior decisions, which may lead to higher equipment failure rates, inadequacy of systems in given circumstances and responsibility for reduced capability of the MCR crews due to poor MCR information and poor training of the crews in the procedures and understanding of plant dynamics. Here the systematic effects on personnel performance are considered, there can of course be other effects which can affect individual operators. It is difficult to predict individual operator performance, especially when a given operator is affected by some external influence, like family problems.

A study of accidents shows the importance of not only operator performance (control room and maintenance) in the evaluation of the consequences of the accident, but also the role of designers and management. Both sets of persons set up the operators by determining the context under which they function. For example, the selection of the shuttle booster rocket design set up the condition for failure when compounded by the poor decision-making of NASA management. Other accidents show that the simple PRA model which assumes the independence of maintenance operations from control issues that is there no interactions between operations and maintenance beyond the fact that equipment is or is not available. In the Piper-Alpha accident and to some extent in the Three Mile Island accident, there is an interaction between the two operations. In the catastrophic Bhopal accident, it

was the actions of the management that lead to the inability of the site personnel to deal effectively with accident and mitigate its consequences.

7. COMMENTS

Several comments should be made with respect to accident studies; these are related to the importance of management decision-making in both the design and operational phases of the plant on the accident progression, and the need of persons involved in accident analyses to be more concerned with what are the circumstances that lead to human errors, PRA methods need to be further developed so that the role of management decisions are more explicitly identified as a significant contributor to the accident progression and for HRA practitioners to be more involved in seeing the impact of plant operations during their work of assessing operator reliability.

Accident analysis can help establish, in the minds of HRA practitioners, that human actions do not exist in isolation, but that the human actions are conditioned by the accident situation. Management decisions can strongly affect the context under which accidents occur; their role is a key element in determining the situation, since people operate with their concurrence.

PRAs must find a way to more directly involve management decisions into the PRA and accident analysis processes. Clearly, the failure rates of equipments are related to past maintenance activities which are related to management decisions related funding and manning. The preparedness of the operational staff is determined by the degree of training that they receive, including access to good experiences obtained using simulators and the quality of these items are directly affected by decisions made by management.

Acknowledgements

Thanks to the many HRA persons for their work in the field to expand our understanding of this interesting field. Some were my co-workers and some are other experts. All have made contributions to HRA and/or PRA.

References

[1] W. D. Cullen (Lord), 1990, "The Public Inquiry into the Piper Alpha Disaster," Vols. 1 & 2, HMSO, London, England (Presented to the Secretary of State for Energy, 19-10-1990 and reprinted in 1991 for general distribution).

[2] Rodgers' Commission, 1986, "Report to the President by the President's Commission on the Space Shuttle Challenger Accident", June 6th, Washington DC.

[3] Anthony. J. Spurgin. "*Human Reliability: Theory and Practice,*" CRC Press, Taylor and Francis, 2009 Boca Raton, Florida.

[4] D. Fennell, 1988, "Investigation into the King's Cross Underground Fire", The Stationary Books, London.

[5] Ashok S. Kalelkar, 1988, "Investigation of Large Magnitude Incidents: Bhopal as a Case Study," Institution of Chemical Engineers Conference on Preventing Major Accidents, London, England.

[6] M. P. Broadribb, 2006, "BP Amoco Texas City Incident," American Institute of Chemical Engineers, Loss Prevention Symposium/Annual CCPS Conference, Orlando, Florida.

[7] Joel Rubin, A. M. Simmons & M. Landsberg, "Total destruction: At least 17 die in head-on Metro Link Crash", LA Times, September 12th, 2008

[8] Sidney W. A. "*Ten Questions about Human Reliability*", Lawrence Erlbaum, 2005, Mahwah, New Jersey.

[9] WASH 1400, 1975. "Reactor Safety Study --- An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, DC.

[10.] J. G. Kemeny, 1979, "The Report to the President on the Three Mile Island Accident," originally published October 30, 1979.