AN EXAMINATION OF FACTORS AFFECTING HUMAN RELIABILITY

D M Hunns*

The case-histories of two industrial accidents are examined together with the human errors which were involved. An attempt is made to deduce the underlying psychological, situational, organisational and cultural factors which contributed to cause them. Common elements between the two accidents are identified and modern safety management techniques are considered in terms of their effectivenesses for preventing such accidents, particularly in the contexts of today's and tomorrow's computer controlled process plants.

(Key words: Human error, accident, causes, prevention, Markham, Abbeystead)

INTRODUCTION

Have you ever heard someone say, "It doesn't matter how well you design and build a system it can only be as reliable as the people who operate it - and people arn't very reliable, are they?"

The second part of this statement is hard to deny. In general, human beings are not very reliable, at least not if considered against reliability levels, say, of better than one error per ten thousand actions. Which is typically the kind of reliability required, and better, if controlling significant hazards. Certain types of action, eg correctly locating one's own house when returning from work, are in this range but in general these make up only a small proportion of the total task-sets performed by humans in real-world operating situations. So, yes, it is hard to argue against the second part of the statement ....

But what of the first part? Do you feel, intuitively, that the statement is too sweeping, too simplistic - above all does it accord with observation - that is, are the frequencies of significant accidents and of 'task-level' human errors comparable? The answer surely is no - the two usually are orders of magnitude apart. But why? What in any system are the real features which determine this difference? Only if these can be identified have we other than a subjective basis for arguing our opposition to the third, and unspoken, part of the opening statement, viz. *"Therefore undertakings involving real hazards can never be safe".*

*Health & Safety Executive, Nuclear Installations Inspectorate, Bootle Merseyside.

This then is the quest on which the Paper embarks, not comprehensively as this would be a considerable task, but in a way which aims to draw out at least one two of the key factors which determine how human reliability influences the operational performance of a system.

There are no better information sources to consult than the investigation reports of actual instances where human error has caused failure at the high system level. The two examples chosen for this Paper are the 1973 Markham Colliery overwind accident and the 1984 Abbeystead explosion. In each case the circumstances of the accident are given, followed by an analysis which attempts to deduce what were the true building bricks of human error and to identify effective blocking strategies.

TWO ACCIDENTS

Markham Colliery

The winding engine of No. 3 shaft was tested every three months by the Area Overwind Testing Engineers and at the time of the accident was certified as complying with the statutory requirements. Nevertheless, on Monday 30 July 1973 at about 6.20am, when 29 men of the first dayshift were descending the 1400 ft shaft, an essential component of this 'tested' system, a 2" diameter carbon steel rod, transmitting braking force from a spring nest to the winding drum, abruptly fractured.

The winding drum carried two brakes constructed on the circumferences of the drum's two circular end-plate assemblies. Each circumference was served by an upward acting Ferodo-lined brake shoe. Either shoe acting alone was capable of supplying the necessary braking action. These brakes could be applied manually by means of a lever in the winding engineman's cabin - also they were subject to automatic operation by a system of protective trips. Additionally, regenerative electrical retardation occurred whenever the winding engineman, during raising or lowering, moved his speed control lever towards 'off'.

The 2" steel rod transmitted the force of an 8ft high spring nest, via a short train of levers, to the brake shoes, the force acting to hold the brakes 'on'. A pneumatic cylinder, acting also on the lever train and under the control of the brake lever in the winding engineman's cabin, served to oppose the force of the spring nest and enabled controlled release or application of the brake shoes. "Ungabbing" gear, hydraulically powered and controlled by the automatic trip system, acted mechanically to disengage the brake lever and vent the pneumatic cylinder, thus causing full application of the brakes.

By 6.20 am on the morning of the accident 105 persons had already been lowered. Another lowering was in progress and all had proceeded normally until the mid-point of the wind. The speed of the cages would then have been about 13 mph. At this point, with the imbalance of weights progressively favouring the descending cage, it was normal for the winding engineman to start retarding the engine.

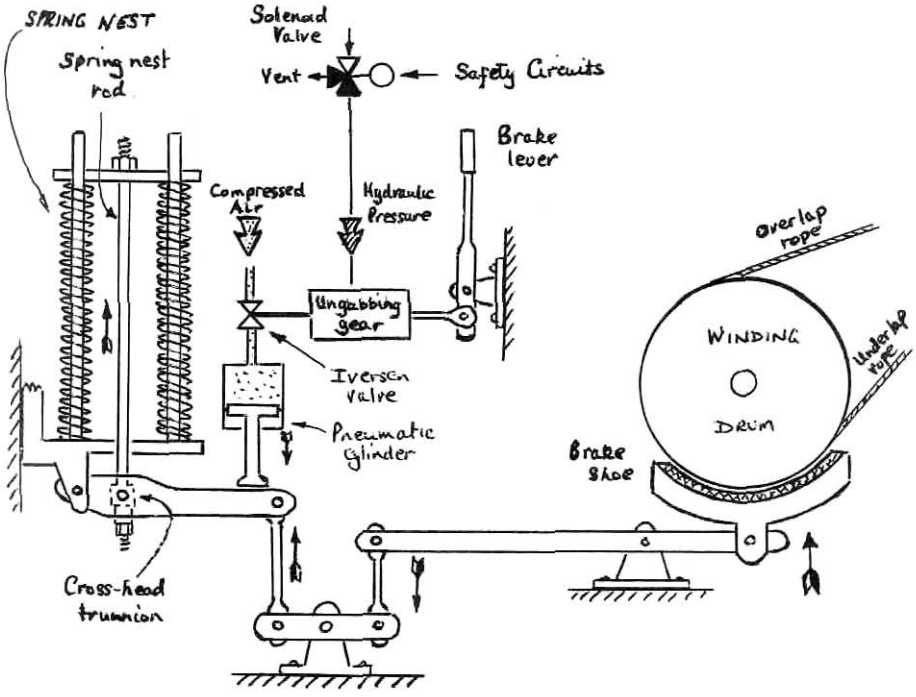


Fig 1 Shematic of Mechanical Braking System

As he began to take this action he noticed sparks under the spring nest and heard a bang. He at once moved the speed control lever towards 'off' and the brake lever to 'on'. The lever, however, felt to be disconnected and failed to have any effect. Hastily he pressed the emergency stop button, a perfectly natural reaction at such a moment but one which, because of the associated tripping of the electrical power to the winding motor, also disabled the regenerative braking action. Thus, the last of the remaining braking was removed and the rotation of the winding drum continued unabated.

His last and desperate act was to trip the hydraulic pump which powered the ungabbing gear - but the braking system, with its main force path severed, was by then beyond recovery and the final tragic outcome already sealed. Within 30 seconds of the engineman discovering his useless brake lever, the descending cage, then travelling at an estimated 27 mph, reached the pit bottom. Eighteen of the twenty nine men were killed and none of the remaining eleven escaped without serious injury.

The accident enquiry concluded that if the regenerative braking action had remained operational, the final speed of the cages would have been significantly reduced. However, it was considered that the action of the winding engineman was above criticism, given the situation with which he had been faced, and the means available to him for dealing with it.....

Analysis

It might be considered that the engineman, by his inadvertent disengagement of the regenerative braking, was guilty of a category of human error known as 'mental model perception failure'. However, his state of mind in those first few seconds must have seen a rapid escalation from sudden anxiety to nightmarish shock. With his brake lever like a broken fence post and the unthinkable possibility of a man-winding runaway he had failed to appreciate that the 'stop button', which until then had always meant 'stop', now traitorously meant 'go'.

When manifestly a fearful thing is 'on', the natural human reaction is to turn it 'off'. This survival response is deeply engrained from early childhood and is virtually irresistible. It is a form of 'pre-experience take-over' and is essentially a reflex error of the non-culpable kind. The true failing, of course, lay not with the engineman but rather with the human team which placed him in that terrible situation - which the accident enquiry properly recognised.

The investigation into the cause of failure of the spring nest rod revealed an interesting design weakness. The rod served to transmit the spring nest force to the "main" lever via a crosshead trunnion, the trunnion axle bearing directly onto pads set into the lever. The bearing pressures thus created were such that any lubricant present quickly became ejected from between the mating surfaces; and since there was no engineered provision for replenishing the lubricant, short of forcible separation of the parts, the virtually permanent condition of the bearings was one of maximum frictional interaction. In consequence a bending force was applied to the trunnion end of the spring nest rod whenever motion was transmitted to the brakes.

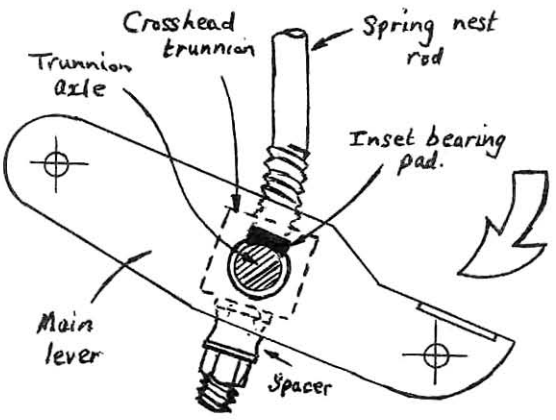


FIG. 2. Illustration of Bending Action.

It was demonstrated that the rod had an adequate margin of strength to cope with the steady tensile stress induced by the spring nest but the designer had not catered for the fatigue burden superimposed by the additional bending cycles. The safety margin here in fact was found to be negative, which meant that eventual failure had always been inevitable. The moment came in that early morning of the 30 July 1973 - 21 years after the rod had first been brought into service.

Undeniably this was a manifestation of designer error although whether through over-sight, mis-calculation or wrongful judgement we cannot know. The lack of an engineered means of lubrication, which would have been an exceptional over-sight had one been intended, might suggest as more probable that the designer had consciously decided against the need for lubrication in the instance. Whatever his presence or absence of motives, however, there is no escaping the fact that the design was flawed.

Such are the interactions, iterations and convolutions of the design process that mistakes, particularly at the more detailed level, are inevitable; and a proportion of such mistakes will survive even the most rigorous of checking regimes. This we must accept. There is, however, an essential and potentially effective last line of defence, namely, the systematic and repetitive testing of 'function' and 'fitness-for-purpose' which must form part of the ongoing life of any operational facility.

Effective proving of this kind requires in every instance that a practicable, dependable and searching method of testing or examination be available. The designer, given that he recognises testability as part of the design requirement, is in the strongest position to ensure that this aspect is adequately provided. In the case of the spring nest rod the designer had made no provisions of any kind.

On 14 January 1961, twelve years before the Markham rod failure, a similar rod broke at Ollerton Colliery. Routine examination of all operational spring nest rods was stipulated from that time but it seems that the method adopted was one of visual inspection, and it was to be later proven that this stood little chance of giving reliable pre-failure warning. More latterly, as was demonstrated during the accident enquiry, ultrasonic inspection could have been used entirely effectively for the spring nest rod - but it was not.

As a broad generalisation, the design of heavy engineering components traditionally adhered to the principle of 'designing beyond life'. That is to say, components were designed with a sufficient margin of strength to guarantee survival during the expected operating existence of the facility. The margin would be such that any defect capable of removing it would need to be so large that its detection, even by visual means, could hardly fail - a persuasive enough argument in principle!

In the case of the spring nest rod the safety factor was 6, but, as has already been noted, this was related to the linear loading expected from the spring nest and did not allow for the additional bending fatigue which the rod also was to experience. Had the designer appreciated the existence of this extra component we must presume that he would have strengthened the rod accordingly. We can be confident, however, that his attitude to in-service proving would have remained unaltered.

That the designer chose a nest of springs rather than a single spring might be construed as one example of where it was felt that 'design beyond life' could not be guaranteed. By the arrangement adopted, failure of a single spring would not disable the braking action and would be visually detectable before other failures followed.

A designer can only make such selective decisions by reference to his life-time learning and experience. Failures of springs would be known and understood; a reality with which every engineer/designer had to cope. However, failures of simple components in simple duties would be much rarer and generally, when they did arise, could be traced to some special reason, perceived as avoidable in the future. Therefore even these 'rare' faults would tend to be seen as 'one-offs', if anything adding to, rather than detracting from, the designer's confidence in future performance.

Confidence in a component's reliability is a complex amalgam, firstly of belief in the design and manufacturing processes from which the component was born and, secondly, of subjective performance expectation, sublimated from education and direct life-time experience. Such a system of conviction must have prevailed to allow that an essential system component in a winding *engine braking system received only superficial examination throughout the* 21 years of its operational duty - until the system itself finally tested the component to destruction. We are not looking at slack practice or at lack of ability or means. We are looking simply at a cultural approach to the attainment of reliability.....

Today, the technique of probabilistic risk analysis is available and this can tell us that a life-time's 'no failures' observation, say over 50 to 100 years, even though embuing the observer with the highest subjective confidence, nevertheless in statistical terms represents a corresponding reliability which is surprisingly poor. For example, a period of 100 years with no observed failures enables us to believe (based upon the Poisson distribution) with 99% confidence that the equivalent failure rate is not worse than one failure per 20 years. This is a dramatic reduction in expectation and, of course, there is still a 1% chance that the situation could be even worse. Given this kind of objectivity, would the braking system designer still have placed all his faith in the 'design beyond life' principle?

Proper application of today's risk assessment methodology, within which the philosophy of full testability is one essential bastion, would have systematically questioned the routine testing/examination of all critical system components, including static members such as the spring nest rod. We cannot claim that the subtle mechanism of the rod's demise would have been uncovered by the analytic process but the efficacy of the rod's testing would. Moreover, an appropriate frequency of proving, related to specified risk, could have been deduced.

Additionally, it may be fairly claimed that the risk assessment process would have found the dependence on so may single components (there were more in a primary safety role than just the spring nest rod) to be totally unreconcilable with the attainment of an acceptably row risk for the man-winding operation. Most evidently this was not the view held by the original designers. But it was the view reached by the accident enquiry which called for the systematic elimination wherever possible of all "single-line" components in this and all similar winding installations.

Firstly we see a winding engineman's error, but one concluded to be of the non-culpable kind - the fundamental failing lay not with the driver, so to speak in the heat of the race, but rather with the designer who permitted the 'stop' button actually to remove one element of the stopping action.

Secondly, we see a subtle design error surviving detection through manufacture and even seemingly, at Ollerton Colliery in 1961, an actual demonstration of its deadly potential. A kind of error which no amount of design review can ever entirely eliminate.

Thirdly, as the logical by-product of an engineering culture, we see the persistence of an inadequate inspection practice for a vital component, despite the later availability of a fully effective means of examination.

Fourthly, and most significantly of all, we see a design embodying over-dependence on 'single-line' components, emphasising again the limitations of individuals' subjective experience as compared with the objectivity of measured analysis.

All the elements of the accident at Markham Colliery stem from a combination of the winding engine system's design and the engineering culture of the industry at the time. Errors undoubtedly were made but in the context of their occurrences it is difficult to attach absolute culpability to any single one - rather, all, in their varying degrees, added their links to the chain which finally became completed so unforgivingly at Markham No. 3.

With proper application of the safety management techniques available today, which include risk demonstration with respect to both design and operational safety, we could hope to avoid a repetition of the circumstances of Markham. The provision of this essential safety net, however, requires the establishment of a dedicated and independent safety organisation fully resourced to scrutinise every stage of a project's evolution and operation - and, furthermore, vested with sufficient authority to exert real influence.

Abbeystead

Contrary to the designer's Manual of Operating Instructions the method of operating a washout valve had become modified, commensurate with a change from periodic batch washout to a practice of continuous washout bleed. The modification meant that the valve, from being kept normally closed, was operated continuously 'cracked' open. Four years later it proved impossible to determine exactly who had authorised the change but it was believed that the motivation had been the avoidance of silt build-up behind the closed valve, and consequent discolouration of the receiving river following the batch washout discharges.

The washout valve operated in parallel with a weir system which, with the valve closed, was designed to maintain the associated 6.6 km water transfer tunnel (a section of the Lune/Wyre water transfer scheme) in a fully flooded condition. By so doing, whether or not this was strictly essential, water delivery could immediately take place whenever transfer pumping was actioned.

Also, as was to be demonstrated by subsequent events, the maintenance of a fully flooded tunnel played a vital safety role. It seems, however, that this second aspect was not appreciated by the operators, or indeed by any of those involved at the time, and little importance was attached to ensuring the tell-tale presence of water flow over the weirs during the routine visits to the valve house. Indeed, with the passage of time and change of operators, the positive confirmation of physical flow over the weirs ceased to be a part of the weekly checking routines.

Thus, two seemingly harmless changes in operational practice had evolved, the first creating real opportunity for the tunnel not to remain fully flooded and the second enabling this situation to persist undetected for a protracted period of time.

In due course the enabling elements of human error were provided - firstly, an erroneous setting of the washout valve which left it slightly too far open, natural chance then exacerbating the position by providing a period of particularly low rain-fall - and secondly, the employment of an operator who, although routinely checking the outfall to the river, had not been instructed to interpret in plant terms, or be concerned by, what he saw; in this case the persisting dry states of the discharge ports from the weirs. His last routine visit to the valve-house had concluded uneventfully only hours before the accident occurred. By this time, as it is now believed, the tunnel had been variously in a state of voidage for up to 17 days.

Unbeknown to the operators and designers alike, a menace from the most ancient of origins, later to be identified as fossil methane, was awaiting this very opportunity. Although known to have low solubility in water under normal conditions, the elevated pressures of the surrounding geological environment altered this situation to the extent that the in-leaking water (more than 1000 m^3/day) to the tunnel carried sufficient of this dissolved methane to create, over the nominal 17 days period, an explosive concentration of gases within the tunnel void. Subsequent pumping of water through the tunnel acted to displace this lethal atmosphere to the Abbeystead end where, by an unfortunate arrangement of ventilation, the discharge was directed into the valve-house.

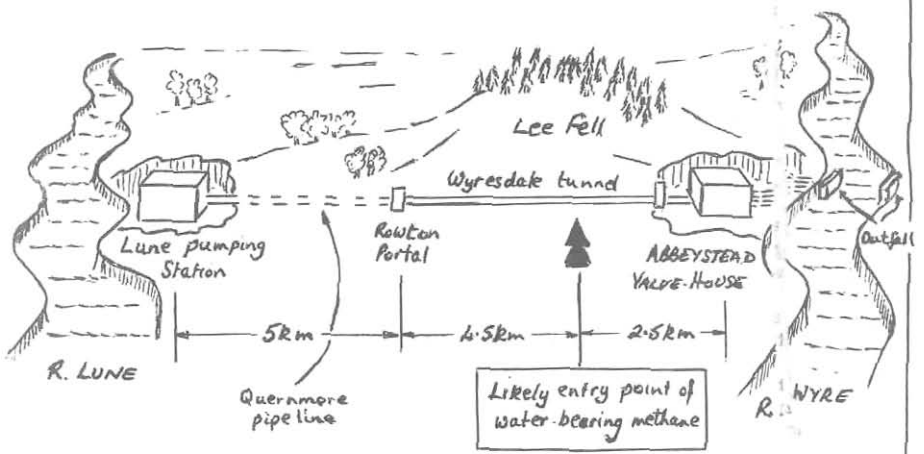
The stage was thus set for tragedy and on the 23rd May 1984 it became consummated. On this fine May evening a party of 44 visitors and Water Authority staff were assembled at Abbeystead and by 7.30 pm most were collected inside the valve-house, waiting while the distant pumps worked to bring water from the Lune. The exhaling tunnel required only to find a source of ignition - and amongst the company were smokers..... In the ensuing holocaust, of those in the valve-house 16 died and no survivor escape injury.

Analysis

To the designers and constructors of underground workings the potential hazard of explosive atmospheres is as much a part of their awareness as is he hazard of electrocution to the electrical power industry. However, whereas the hazard of electrocution is always present, the explosive atmosphere hazard is more quixotic.....

The geology of the area through which the tunnel was to pass was particularly well known but Binnie & Partners, the pumping scheme designers, although they investigated the geology at the tunnel ends, did not extend their bore-hole explorations to include the deep line of the tunnel. Based upon past experience, they had concluded that the extra information gained would not have justified the effort and cost of its procurement. It seems that water ingress, rather than gas ingress, was the main practical difficulty anticipated.

FIG. 3. Schematic Arrangement of Lune/Wyre Water Transfer Scheme



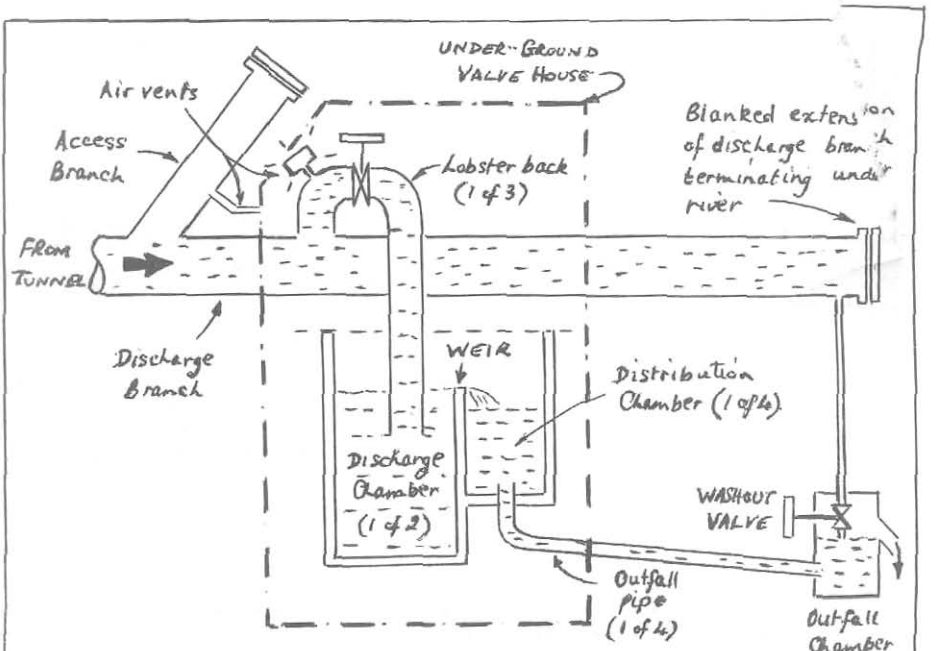


FIG. 4. Illustration of Abbeystead Discharge System

During the tunnel construction the standard precautions against flammable atmosphere formation were taken but at no time was methane detected to any significant extent. The fact that the design positively catered for a fully flooded tunnel might suggest at some point an element of quiet cautionary thought, but, if this had been so, we must logically suppose that the designers would have ventilated the tunnel directly to atmosphere. In fact, not by omission but seemingly by positive provision, the tunnel was ventilated directly into the Abbeystead valve-house; moreover, if any serious possibility of methane had been anticipated, intrinsically safe electrical equipment would have been installed in this below-ground building and possibly also a methane monitor provided. The facts provide their own statement; such features were not incorporated.

The evidence of the exploratory surveys, the general experience of this type of geology, the detailed design, construction and subsequent operation of the water transfer scheme all point relentlessly to the one conclusion, namely that the gas explosion hazard, although passingly investigated, was not a factor carried forward into the project. The designers had anticipated water ingress but they seemingly had not recognised that such water, emerging from a higher pressure environment, could contain significant amounts of gas not appreciably soluble under normal conditions. Such knowledge was not common in the industry and the continuously ventilated state of the tunnel virtually throughout the period of its construction would have masked any manifestation of the effect.

Clearly there were operational irregularities, notably the too easily made changes in the washout practice and in the level of surveillance applied to the valve-house operating conditions. Seemingly these changes were made for reasons of local convenience without any formal reference to the possible wider implications. This was wrong and revealed a flaw in at least one aspect of the North West Water Authority's management of safety. However, even had the implications of the changes been formally questioned, right back to the designers, it is very doubtful whether the methane hazard would have been a guiding factor in any response. Simply in this case methane was not a recognised danger.

Must we therefore conclude that the Abbeystead disaster was unstoppable? After all, the root cause in the whole chain of events was the unawareness, by experts, of methane as a potential hazard in this particular case. From the outset methane had been judged as an unlikely candidate for concern and the tunnel construction phase had appeared to verify this expectation.

But here perhaps we touch on the achilles heel of the whole enterprise. This final verification, the test measurements, as reported, were not truly rigorous. Of ten known measurements made only one was conducted without the ventilation system being in operation and, even in this case, the period from shutdown is not stated. Furthermore, the instrument used, a Draeger gas detector, in the circumstances of its use would have yielded only the crudest indications of specific methane presence. As well, it is almost certain that when the measurements were made the safety concerns of the constructors would have been centered on the construction phase itself, not on the tunnel's operation. Anyway, it would be known that the intention was to operate the tunnel continuously flooded. Fire and water do not cohabit. Methane absent or present, and it was believed to be absent, sounded no alarms for the future - once the tunnel was built.....

So, these crude measurements, while serving their immediate purposes, were incapable of providing the longer term assurances which we now know were just as important. The constructors were working to their normal agenda - and the vital item under 'Any Other Business' had not been included..... After all, the tunnel was to be kept flooded.... and if flammable gases were around the constructors would let us know.... But "no news" is not always "good news". *Seemingly the matter proceeded on a fabric of negatives while what was* missing was the single 'positive' - "Demonstrate that an explosive atmosphere cannot form". And to pose such a challenge, by the very strength of its niaivity, may require a certain independence.....

The cause of the Abbeystead disaster was therefore rooted in an erroneous design expectation and a failure to employ effective means for verifying this expectation. It is fair to claim that the use of independent risk assessment, systematically applied, would have stood a high chance at least of questioning this issue; and may well have applied the required 'positive' by emphasising the need for specific test verification in relation to flammable gases. Effective quality control, exercised within a structured 'safety management' regime, would have examined the appropriateness of the test verification method and perhaps these challenges, acting together, would have blocked the pathway to tragedy which ended in the terrible events of that fine May evening in 1984.

CONCLUSIONS

The two case-studies presented involve different industries and quite different technologies. The natures and forms of the disasters which they involved also were different. The broad equivalences which can be drawn from their causal patterns of human error are therefore all the more remarkable.

Firstly, in both cases the basic cause was designer error, but of a kind whose potential can never be eliminated. At Markham, a number of design weaknesses perhaps the primary one of which was the dependence on "single-line" components. At Abbeystead, the premature discounting of the potential flammable atmosphere hazard.

Secondly, the failure of the principle safety net, that is the failure to recognise, and provide for, the positive proving of a safety related component, function or assumption - again attributable as design error but bearing influences of the culture of the industry. At Markham, the lack of an effective inspection method for the spring nest rod. At Abbeystead, the failure to apply an effective test to confirm a design assumption.
Thirdly, operator/maintainer error but of the kind which naturally emanates from the pressures and circumstances which the design errors have pre-determined. At Markham, the winding engine-man's removal of the regenerative braking action. At Abbeystead, the informal modification of laid-down operating instructions and the failure combination which produced, and allowed to persist, the partially drained state of the tunnel.

It is considered that the formal application of techniques such as Hazard & Operability Studies and Probabilistic Risk Analysis at the design stage of both undertakings, by their structured and systematic approaches, would have challenged most of the factors which under-pinned the accidents. They would have called for justification of the initial assumption at Abbeystead and would have identified and analysed the 'single-line' dependence at Markham, and offered a quantitative assessment of system risk.

The power of such techniques derives from the independent and systematic examination which challenges the designers not only to create systems of calculated reliability but also that they should formally demonstrate that they have done so. It requires also that safety cases be documented and that their assumptions and defining parameters be carried forward into the system operation as operating rules/instructions.

Furthermore, there needs to be a readily traceable and documented relationship between each operating rule/instruction and the hazard to which it refers. Managerially there must exist a formal means whereby any proposed alteration to an identified safety-related instruction/rule is assessed in relation to the safety case before it is adopted. Such a system was not operative at Abbeystead.

Finally, it is again stressed that the responsibility for effective system proving, whether routine or otherwise, starts with the designer. In the same way as he designs for operability and maintainability so must he design also for testability.

By far the greatest human error contribution in both of the accidents analysed was designer error. Operators will continue to make errors day by day. This is a fact of life. But it is the designer who sets the scene, who must seek to include the defences needed to make the operation tolerant of such errors. Where his efforts are deficient, the operator 'in the front line' sooner or later will be beaten.....

If the seeds of destruction can survive elimination in a traditional colliery winding engine and a simple water-works, how must we regard the possibilities for a large computer controlled chemical plant? The 'programmable logic controller' in its many forms is now the typical nerve center of such plants and commonly will be found operating not singly but in sophisticated networks of distributed intelligence.

The important physical change introduced by this technology is the replacement of hardware by software for the implementation of control functions and information management. It is, however, the resulting step-increase in scope for the inclusion of extra dimensions of automation which has been both dramatic in effect and irresistibly impressive. But this means that from the point of view of the safety analyst he sees a control regime of vastly increased complexity with considerable scope for in-built, or subsequently introduced, errors. Moreover the embodiment of the associated logic is relatively covert. The analyst's task of demonstrating safety, where automation of this type and complexity is involved, becomes highly demanding and almost inevitably destined to produce less than convincing results.

Nevertheless the principles highlighted by the two accidents studied should not be ignored, namely (i) the need for the designer to provide for, and ensure, the positive proving of significant safety-dependent assumptions, (ii) the need for the designer to make the necessary provisions for the thorough routine proving/maintenance of safety-related systems and components during normal operational life, and (iii) the need, where significant hazards are involved, for the making by independent specialists of a documented safety demonstration. A fourth might be added: (iv) the need for designers to confine their designs to forms which allow effective safety demonstration.

The latter need presents a particular challenge, for where major hazards are (or might be) involved it is no longer enough simply to design for safety and allow that history will prove the case - today, such safety must be demonstrated in advance, and the associated designs, irrespective of sophistication, must remain amenable to this requirement.

REFERENCES

CALDER J W, 6 March 1974, Report on the cause of, and circumstances attending, the overwind which occurred at Markham Colliery, Duckmanton, Derbyshire, on 30 July 1973, HMSO, HM 6602 Dd 252561 K32 3/74.

Health & Safety Executive, 1985, The Abbeystead Explosion, HMSO, ISBN 0 11 883795 8.

V/NII.D1./D7/02.89/SAH