LINKS IN THE CHAIN – A NEW PARADIGM FOR THINKING ABOUT SAFETY

Dominic Irvine[1] and Glenn Sibbick[2]
[1]Managing Partner, Epiphanies LLP, 4, Lenten Street, The Old Bakery, Alton, Hampshire, GU34 1HG, UK;
e-mail: dominic.irvine@epiphaniesllp.com
[2]Operations Director, Centrica Storage, Unit One St Augustines Park, Hull Road, Hedon, East Riding, Yorkshire, HU12 8QN;
e-mail: glenn.sibbick@centrica-sl.co.uk

The cause of many incidents in the oil and gas industry is the cumulative effect of multiple 'micro' decisions that people take the effect of which is a catastrophic failure leading to injury and sometimes death. These human factors in the cause of incidents are managed through an ever growing array of processes and procedures. The paradox is that the effect of these processes and procedures is to so stymie production that operators have to employ 'temporary fixes' or 'workarounds' in order to keep their operations working. These 'temporary fixes' have an additional undesirable effect of negating the value of the processes and procedures. Ultimately, the industry will become clogged by the increase in processes and procedures. This article proposes that what is needed is firstly; a shift in the mindset of operators from a standard risk based analysis to a consequence based understanding: Secondly; the creation of a 'highway code' for operational staff akin to that used by road users: Thirdly; creating the right consequence driven context to drive the desired behaviour. The outcome of these changes should in the authors view provide an alternative way of thinking about safety that reduces the dependence on ever more processes and procedures.

INTRODUCTION

There are some fundamental assumptions that underpin current thinking on safety that we believe to be flawed. The pervasive pressure to operate safely for the benefit of the worker, colleagues, the asset and the company is inadequate at preventing the micro decisions that workers take on a day to day basis that compromise safety. By this, we mean those decisions that are taken without reference to the whole system.

We present a new paradigm to thinking about safety and with this in mind, offer a different approach to achieving a 'safe operation'. Our credibility is based on the experience of one author as a Director of Operations for the North Sea Rough Storage Facility within the UK continental waters. The other author has many years of experience in designing and delivering behaviour change programmes for a number of FTSE 100 companies. These backgrounds supported by insights from relevant literature underpin the analysis presented.

We set out first the cause, of almost all incidents. Secondly, we examine the current response to the lessons learnt from such incidents to reduce or eliminate similar incidents occurring elsewhere. We conclude with an alternative approach to how safety should be addressed.

The infrequency of incidents in the oil and gas industry is testament to the success of safety campaigns, education programmes and changes in legislation. The solution thus far has been to add ever more processes and procedures into the way work is done to ensure what is done is done safely. However, as systems become ever more complex and interlinked, the ability to prescribe a set of procedures for most eventualities has led to the production of complex operating and incident procedures focussed upon management at a single process and procedure level. Often, these procedures fill several lever arch files with information the duty manager is expected to understand and follow.

CURRENTLY

The process and procedures are designed to maintain safe operations and allow maintenance. Essentially, the belief is that the more procedures you put in place, the less probability of an incident occurring i.e. is linked to reduction in risk. Whilst in isolation each process and procedure is deemed to be safe, little account is taken for the macro impact of many micro level procedures being implemented. The impact of multiple variables on the integrity of a system is too complex for an operator to ever be able to understand, but yet the operators may make a series of what are assumed to be unconnected decisions over time to implement a number of micro level decisions to inhibit a process or procedure to achieve a specific end.

It is these decisions people make that are critical, as Reason (2000) shows in his analysis of the incident at the Chernobyl Nuclear Reactor.

> *At Chernobyl, for example, the operators wrongly violated plant procedures and switched off successive safety systems, thus creating the immediate trigger for the catastrophic explosion in the core. Followers of the person approach often look no further for the causes of an adverse event once they have identified these proximal unsafe acts . . . virtually all such acts have a causal history that extends back in time and up through the levels of the system.*
>
> (Reason p. 768)

Similarly at Texas City the operators also violated plant procedures and switched of successive safety

systems. On March 23rd 2005, 15 people were killed and over 170 harmed as the result of a fire and explosion on the Isomerization plant (ISOM) at the BP Products North America owned and operated refinery in Texas City, Texas, USA. (p. ii)[1]

In this incident, a team of experts struggled to determine the exact cause and sequence of events that lead to failure. Yet, those operating the facility believed they were making the right decisions at each stage of the incident based on their knowledge and previous experience without understanding the broader impact each decision had on the macro picture in a rapidly developing and changing event. The lack of awareness of the effect of the changing state of all the variables was not understood. Successive decisions were made and each of these seemed sensible at the time. This combination was catastrophic.

Where the conclusion reached from analysis is that the probability of an incident arising from a specific circumstance is low, mitigation against the incident tends to be procedural and superficial rather than an engineering solution, generally, for the expedience of cost. A procedure carries with it the additional costs of training and rests on the assumption that someone trained in the procedure will then follow it each and every time. What happens currently is:

> *. . .methods like HAZOP (hazard and operability study) or FMEA (failure mode and effect analysis) are applied with an analytical view consisting of decomposing the installation into parts and of identifying what cause-effect relationships could lead to hazardous sequences.*
>
> (Le Coze 2005 p. 623)

This in turn leads to engineering and operational process and procedures to prevent those causal effects from arising. Unfortunately, people and organisations cannot be adequately broken down into a series of steps such is the complex interplay of the variables involved (economic, cultural, political etc.). Alternative perspectives are required (Le Coze 2005). It is possible to predict a time where the complexity of systems is such that the level of process and procedure required eventually so stymies work that either the workers sidetrack the safety process. Or they potentially fail to deliver their fundamental objective of keeping the operation running.

It is the use of 'temporary fixes' that is symptomatic of the mindset issue at the heart of the problem. Examining the existence and use of temporary fixes will illustrate the need for the different way of thinking that is proposed later.

TEMPORARY FIXES

Safety critical elements (SCEs) are:

- A safety critical element is a piece of equipment that protects the plant
- Failure of which would cause or contribute substantially to an event.

When maintenance is done, an SCE may be inhibited to allow maintenance to take place. That inhibit which allows an operator to sidestep a range of procedures or processes and hence maintenance to take place can become a 'quick fix' to a problem enabling operation to continue. On the basis 'if it worked once it will work again' a temporary solution becomes a 'permanent fix'. What seem to be logical, sensible and pragmatic 'work-arounds' crop up frequently in the analysis of major incidents. In the fire and explosion at the ConocoPhilips Humber refinery on 16 April 2001, the injection of water into a system to reduce fouling led to the erosion of an elbow on a piece of pipe work which subsequently failed.

> *The modifications had the hallmarks of a 'quick fix' to solve the symptoms of the immediate problem of fouling . . . This perception of a 'quick fix' is supported by the failure to implement the MoC [manage of change] system in operation at the time that would have required a technical memorandum to be raised covering the modification.*

An examination of the fire and explosion in Texas paints a similar picture of lack of understanding of the consequences of a short term 'fix' to solve an immediate problem. As with the Humber refinery incident, the investigation team "found no evidence of anyone consciously or intentionally taking actions or decisions that put others at risk." (p. ii). In the analysis of these and other incidents, it is clear that for every procedure and process put in place, people will find a temporary fix that allows them to get the job done. The consequences of these decisions can be catastrophic, but it is not the consequences people are asked to address, it is the risk. This factor is addressed in more detail later. Given the use of a temporary fix is so well understood as a cause of incidents, why do operators still persist in their use?

THE WAY OPERATORS TAKE DECISIONS

Operators make decisions based on small amounts of training and a wealth of experience. They are not engineers or physicists, or chemists, technical safety engineers, lawyers or operations experts. On site, problems are identified at a micro level. The operator embarks on an action to put on an 'inhibit' and follows a procedure to do this. An inhibit is an action to override part of the safety mechanism. They are often used in maintenance work and occasionally during production. The operator may falsely assume that because nothing has happened at a micro level that the system remains safe. This assumption rests on the belief that all other factors will remain constant and be unaffected by the impact of the decision taken. But they cannot possibly know. The point about using 'inhibits' is that they override the design created by the original multidisciplinary team of

[1]http://www.bp.com/liveassets/bp_internet/us/bp_us_english/STAGING/local_assets/downloads/t/final_report.pdf

experts, necessarily so, because of the need to solve a specific issue at a point in time. Inhibits are meant to be a 'temporary fix' but they are also another link in a chain of events.

The implications of procedures and processes do not require the operator (nor could they) to look at the macro picture. So multiples operators making micro level decisions following procedures means there is no overall macro understanding of the impacts of all the decisions.

The danger is when people take an action at the micro level they believe to be safe but whose consequences are unknown or thought so unlikely to happen as to be irrelevant. For example, in the Connocophillips incident the injection of water into a pipe to clear residue destroyed the protective layer lining the pipe. To have known this would have required:

1. The design of the pipe's protective system be understood
2. The limitations of the design
3. Ensuring what was a 'temporary fix' does not become a permanent solution

The chain of events that forms is unseen. All each person sees are the specific micro level detail of the decision they made. Chance dictates whether an activity undertaken at one moment in time impacts on an activity undertaken somewhere else to create an event or incident. Like ships passing in the night, two decisions may come perilously close to colliding but never quite touch, or remain miles apart. In the clear light of day, and with the benefit of hindsight, the proximity of events leading to failure is plain to see, but from the immediate perspective of the operator making decisions in the heat of the moment, there was little or no understanding of the consequence. As the saying goes, 'a miss is as good as a mile' except where the operator bases future decisions on that miss being a mile and therefore legitimizes repeat behaviour.

To understand the chance of something happening requires you to a) know the what that something is and b) be able to make an estimation of its impact, i.e. its consequence.

From our experience of the analysis of major incidents there are a wide range of circumstances in which following procedure is not done for what prima facie seem logical and sensible reasons. For example, an operator emptying a tank to the required threshold presented with two different readings from two gauges may decide to follow the evidence of just one gauge because it confirms the level expected. They decide the other is faulty. Then the operator decides that as one level is faulty to inhibit its 'effect'. If nothing happens the assumption continues that all is well. It may also give the operator more confidence to make similar decisions. The operator can also fail to see the significance of the application over time as the only evidence s/he has is that at the point of application 'nothing adverse happened'. This therefore reinforces the feeling of success and of perceived positive learning. In actuality, the operator has no way of knowing whether they missed by an inch or a mile the causation of a major incident. What started as a temporary fix becomes permanent as the assumption is that the future is largely going to be a replication of the past. Because the tank didn't explode last time why will it this time? An example of a temporary fix becoming permanent is the temporary solution of using a bit of string to keep the gate shut when the hinge has dropped. Because the string works, and the intention is always to fix it sometime soon, it is seen as temporary, but as the years go by it is to all intents and purposes, permanent. Your strategy is what you do, not what you intend to do. Most major incidents seem to be caused by a contribution of multiple temporary fixes becoming permanent solutions.

CURRENT SOLUTIONS

Process and procedures are believed to be the solution to mitigate against the risk of incident. The difficulty is that most incidents occur because of multiple failures linking together. Reason (2000) described it somewhat more abstractly in his now famous "Swiss Cheese Model". The essence of the model is that the holes in the cheese are continually opening up and closing and shifting in location. When momentarily a series of holes opens such that the holes are aligned the circumstances can lead to a catastrophic failure (Reason 2000, p. 7 68). Fundamentally, people are at the heart of the issue be it a mechanical failure or a process failure as both are the product of human activity. The machine did not simply 'exist', it was designed, built and commissioned by people. Therefore the duty manager stands little chance of following correct procedure in the event of a critical failure. This is because:

> *The vast majority of catastrophes occurring nowadays is [sic] generated by the combination of many small events, system faults and human errors, which, individually, would be irrelevant, but, which when combined in a special time sequence of circumstances and actions, can lead to unrecoverable situations.*
>
> (Cacciabue 1998, p. 97)

The outcome of unanticipated events occurring requires new processes and procedures. The creation of these new process and procedures follows the original safe design and each process and procedure in turn is therefore believed to be 'safe'. However the same process of testing to the standard to which the safety process and procedures were originally developed is often not done. One-off unanticipated events can occur which are deemed to require a simple procedure, done once to solve a specific problem. These new procedures are often written at a micro level for micro problems. Because they are viewed as temporary, their impact is not always deemed necessary to undertake the same level of analysis that a permanent solution may require.

Part of the problem is that those who have to deal with the risks and the dangers daily are not those who make the

informed decision about what is an acceptable risk and how it should best be managed. There is a disconnect between those involved in designing and planning the safety systems and those executing the processes and procedures.

The different levels in organisations are responsible for different levels of decisions and work with different levels of details. Boards of companies focused on delivering shareholder value may opt for 'across the board' cuts in expenditure. Whilst financially an expedient move, how it becomes translated throughout the organisation may not be so clearly understood. Pressures on cost make procedures an attractive option over expensive engineering solution for those operating the asset. These decisions are made in 'good faith' but with little understanding of cognisance of ever more reliance on human factors to manage the situation of impending disasters. Decisions about managing risk are made by managers in the safety and comfort of an office, sometimes far removed from the operator who has to make the solution work. Procedural solutions are based on a number of assumptions such as the appropriate provision of training in the new procedure; transferability of skill from one person to the next; close control over variance to the procedure and that there are no unforeseen events which render the procedure partly or wholly ineffective.

The paradox is, as Reason (2000) points out, the very people who are taking decisions with unknown and in some cases unknowable risks are those that afford the best opportunity for operating a safe system, more so than endless lists of processes and procedures.

> *In high reliability organisations . . . it is recognised that human variability in the shape of compensations and adaptations to changing events represents one of the system's most important safeguards. Reliability is "a dynamic non-event." It is dynamic because safety is preserved by timely human adjustments; it is a non-event because successful outcomes rarely call attention to themselves.*
>
> (p. 770)

The operator may struggle to perceive the macro consequence of what could happen because they cannot see the links between what they are doing and others are doing and the major incident that may arise from their decisions. Yet, an operator is in the position of making a great many decisions and choices that can affect the integrity of the system. They can't see because the knowledge and experience they have, has not given them this insight, therefore they believe the decision they take to be safe. Because they are working at a micro level, the experience they have previously is all based on conditions at a given moment in time. The assumption is the future will be a replication of the past i.e. their experience. Experience only has currency based on the future being a replication of the past and that the past is applicable to the future. Experience however does not equal competence.

The links the operators put in the chain are often insufficient to cause an incident not because they know this, but because chance has dictated that insufficient links have formed. It is Russian roulette, where the true level of risk is hidden behind an illusion of safety built upon process and procedures whose credibility rests on assumptions that are fundamentally flawed.

THE NEED TO THINK DIFFERENTLY

The trend towards more and more processes and procedures to drive safety is in our view likely to have the opposite effect to that sought. In short, it will increase the number of incidents. This viewpoint is based on the assumptions that:

- To focus on eliminating as much risk as possible is to approach the problem in the wrong way. In our view, maintaining safety is a dynamic process focused on continually preventing 'small fires' escalating out of control. These fires or safety failures are continually occurring. It is a viewpoint that rests on uneasiness and uncertainty rather than complacency bred through measures of competence.
- People don't understand risk but can appreciate but don't always recognise consequence. A risk based approach is incomprehensible to almost all.
- The disconnection between those taking the decisions about risk and those implementing the decisions drives failure.

We believe people have to know that they don't know the true impact of what they are doing, and therefore have to be mindful that any change will have unintended consequences either positive or negative. We believe that often no-one is necessarily tracking the broader picture and understanding the impacts that each of the decisions has on the overall safety (they just think they do).

RISK VERSUS CONSEQUENCE

An industrial production site can never be truly safe, to achieve this would mean having no system or asset in the first place. Therefore there is always a level of risk. Think about it in terms of continually having to reduce risks all the time. It's an active process. It's analogous to the kitchen in a restaurant. Without regular cleaning, bacteria would grow and the likelihood of food poisoning would increase. Cleaning can never stop, the kitchen will never be clean, but the battle is on to minimise the level of dirt and the likelihood of producing contaminated food. You might be able to sterilise the whole of the kitchen, but the moment food production starts again, bacteria is reintroduced into the system. Therefore the constant state is one of continually striving to keep the levels of bacteria down, not to stop cooking. In the same way, a completely safe asset is one that has stopped producing. The moment you introduce the product, the battle becomes continually striving to keep each part of the system operating within acceptable limits, but not to stop producing.

Each and every action carries with it either a contribution to the level of risk or a reduction. From washing ones hands before handling different types of food, to wiping the surface down; or from raising a permit to work, to maintaining the valves on a gas safety system. Therefore to think about making it safe is misleading. It's about making it less risky. The difficulty is people don't understand risk.

Risk is about chance and its likely consequence; the chance of something happening. Chance is measured by probability; the probability that an event will happen. Risk should not be confused with danger. Danger is about possibility and risk is about probability.

Imagine the sea around an offshore gas platform. Around the platform are barriers and signs which warn you of the 'danger'. They don't provide an indication of what the probability of an accident is, just that the sea is dangerous. No one need fall into the sea for the sea to be dangerous. For example, skydiving is dangerous, in that leaping out of a plane 10,000 ft in the air is dangerous but the probability of an accident is very small. In other words, it's not very risky.

People struggle to estimate risk. The consequence of this is that they take riskier decisions than might be expected and become overly concerned when the risk is small. This can be witnessed in the annual crop of health scares whose statistical risk is small but whose consequence is all apparent. People understand the danger but not necessarily the risk. The Ebola viruses are extremely dangerous, but the probability or risk of becoming infected for most of us is slight. It's easily illustrated by asking yourself how likely you are to have an accident driving your car. You would probably respond, "highly unlikely" after all you're a good driver, right? For your information, there are 317 casualties per billion kilometres driven (Transport Statistics Great Britain 2007). Helped much? Probably not. It's a good illustration of the difficulty of attempting to understand risk at an operational level.

Despite the volume of evidence from a wide range of disciplines over a long period of time (e.g. Slovic, Fishoff and Lichenstein 1979, Thornton 2003) that there is a poverty of understanding about the significance of risk, risk is still used as the principal vehicle for explaining danger. The worker who fails to wear his safety glasses may know that there is a significant risk of sustaining an injury to his eye (Henderson 1991) but still persists. As Thornton (2003) notes:

> *Apparently irrational influences and considerations exert strong pressures. Individuals' perceptions of risk, and attitudes to it, may lead them to choices that seem irrational to the health professional. Perceptions are built up over time, informed by personal experiences and social networks, and shaped by behavioural norms and media reporting*.
>
> (p. 693)

Similar effects can be seen in exercise and diet campaigns. Despite the knowledge that we are at greater risk of heart disease through poor diet and lack of exercise, millions of us still fail to achieve the minimum level of activity required each week.[2] In another example, the popular perception of climbing as a dangerous activity leads many attending management development programmes in which an experiential activity involving climbing is used as a vehicle for learning to experience a sense of fear and trepidation. Yet the reality is that they are at greater risk on the journey to the centre than they are undertaking the activity! (Irvine and Wilson 1994). Most operators know and understand that decisions made operating an asset can have devastating consequences but continue to use inhibits because they genuinely believe that it won't happen.

It is the combination of lack of understanding about the risks, combined with the use of what are perceived to be low risk 'temporary fixes' that provides the greatest challenge. Whilst one fix may be tolerated, the cumulative effect of different 'temporary fixes' in the system, some of which may not be known to all, can be disastrous, as the Texas incident showed. Changing one variable in the system can impact in hitherto unidentified ways, changing multiple variables is almost impossible to predict without the use of complex modelling tools. Such tools are not available to the operator faced with rising pressure and conflicting data on two gauges. The decision is made in the heat of the moment based on previous experience, some actual knowledge and a broad range of assumed knowledge the credibility of which is based on little more than gut feel or anecdotal evidence.

We are missing a trick in focusing on risk. It may be better to focus purely on consequence, i.e. the outcome of the risk. Understanding the consequences of an action is linked to understanding both the benefit and the danger.

For example, the risk of being caught speeding by a camera may not be well understood but the consequence of three points on your driving licence and the impact that could have are much better understood. As a result, the driver going through the camera does not require a supervisor to check his progress because a) the machine does and b) the consequences are very clear. Similarly, the risk in terms of probability of getting one's sleeve caught in rotating machinery may not be understood, but being sucked into the machine and crushed to death is much easier to understand.

Thus, the issue for safety is not so much in helping people understand the probability of their action contributing to a major incident but the consequence of their action. In such instances where the activity is safety critical but the immediate consequence may not be so great, it may be necessary to introduce a substitute consequence of significance because it is the cumulative impact of lots of little steps that leads to the catastrophic failure.

[2] http://www.healthscotland.com/documents/browse/519/1746.aspx

LINKS IN THE CHAIN

We can help provide a better safety mindset by thinking not about making things 'safe', but by thinking in terms of making it less risky. The former is a passive state, the latter a dynamic state. A dynamic state better reflects the environment in which people operate. We then need to link 'making it less risky' with the consequence of what could happen if you don't.

It is useful to think of ensuring safety not so much as the prevention of failure of components or systems or procedures but instead as the prevention of ensuring individual incidents or decisions do not link together to form a chain of events that lead to a disaster. It is clear that all levels and individuals in the organisation have the ability to place a link in a chain. Each individual may not realise the links the others are placing in the chain, or that exist through unknown design failures. Given the increasing complexity of variables involved at any moment in time, it is almost certain that incidents and decisions are regularly forming chains of events that could lead to an incident. By ensuring the chain is never complete so the disaster is averted. Thus each action or decision is either a contribution to an incident.

> *The process leading to an accident (loss event) can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values.*
>
> (Kontogiannis 1993, p. 266)

. . . .or each decision can contribute to making it a less risky place to be.

The choice of whether to wear safety glasses all the time or to 'break the rules' is an issue of helping prevention of the formation of a chain of events leading to an incident or to place another link in the chain. How many people have used their garden strimmer at home without using glasses? Because the consequence hasn't been realised by them so it's deemed unlikely and acceptable even though the consequence could negatively impact their whole life. The distinction between the control of failure versus ensuring adequate constraints is a fundamental shift from attempting to eliminate every possible opportunity for an incident occurring to sufficient feedback loops to ensure small incidents cannot develop into a larger issue.

In any task there is a possibility of an incident which is therefore an issue of managing events to reduce the risk to an acceptable level. If it is a complex task, then the number of issues is huge and cannot possibly be designed out of the operation. It is then a responsibility of all actors in the process to take responsibility for ensuring they keep breaking the chain of events that could lead to an incident. The motivation not to break the chain is driven in part by the perception of the significance of each action and also the assumptions that underpin what might happen.

For example:

> *It's Friday night, it's been a long day at work and Joe is hungry. Driving home, he calls his wife to discuss what they are going to have for dinner. Meg, his wife, is tired too, she's had a long day at work and suggests Joe picks up some fish and chips on the way home as a 'treat'. Both of them know too many chips are bad for you. Both of them know that it's something to do with the fat and it's linked to heart attacks. But they buy the chips anyway, because they don't have them that often and they didn't have a heart attack the last time they ate them. In isolation, one bag of chips won't hurt. [It provides a 'temporary fix' for the need for food quicker than the time it takes to prepare from scratch.] The day before, the sandwich shop was doing a special deal on 'Brie and cranberry' sandwiches, and Joe had treated himself to one. A couple of days earlier, Joe had had a celebratory meal with his boss and had a delicious chocolate tart with fresh double cream. All of these were 'one-off' incidents, and in isolation none were bad. But when the pain spread across the chest and down his arm, and the doctor informed him that Joe was having a heart attack, probably linked to a build up of cholesterol, Joe was shocked. Just as with operators, the failure to understand the impact of multiple micro level decisions had resulted in the system failure where each decision in isolation seemed entirely reasonable and justifiable.*

Given the example of Joe, one to which probably most of us can relate, why is it we expect operators to make the right decisions that take into account the broad picture and understand how a decision at one level can have unintended consequences at another level? Why do we think operators have a level of capability greater than most of the population to be able to translate understanding into behaviour?

We are all putting links in our own personal chains of failure. Think about your own home, somewhere in your house will be an extension socket that converts one wall socket into four additional sockets. Not many of us bother counting the load we have plugged into the sockets. Have you? In so doing you have put a series of links in the chain.

DEVELOPING A SAFETY CULTURE

Given the complex nature of most industrial operations, it is unrealistic to only employ those whom have technical expertise in every discipline. Nor is it realistic to expect everyone to be trained in risk assessment of complex processes. Most shareholders would baulk at maintaining an overhead of technical experts available 24 hours a day, 365 days of the year. In contrast, more often than not, outside of the 9 am–5 pm working hours of managers, key

management support is a senior manager at the end of a mobile phone. At the other end of the spectrum, complete automation of the whole process is beyond what is both technically possible and or affordable. On the other hand, the vast escalation of processes and procedures is stifling the ability of operators to do the work. More processes and procedures cannot be the answer. Given all of this, it is essential that if people are involved in the process they understand very clearly when to 'stop' and or seek further assistance. This is a combination of practice in both safe operations and safe survival following an incident and an awareness of the key triggers that indicate which learnt process to follow. It begins by shifting thinking from risk to consequence.

What is needed is a trigger point to stop the point of escalation. In the example used, this would stop the escalation beyond the fuse blowing. Trigger points depend upon knowing and being fearful of the consequence and not as is currently the vogue, to talk about risk.

The operator should be encouraged to continue making decisions that are acceptable to the level of risk tolerable to the business but should be stopped from making risk decision that are higher than this. To which one could retort 'well I would if I knew what risks he was taking' and hence the need for specific training and development based on understanding consequence.

There are two aspects to developing a safety culture that need to be addressed. How people learn about the culture in the first instance and secondly how this is maintained. The culture needs to be appropriate to the level of risk.

In a very thorough literature review, Lund and AarØ (2004) determined that there are three categories that when brought together have the greatest impact behaviour that minimizes the risk of accidents and injuries.

> *Attitude modification: attitudes are changed by means of persuasive messages in mass media campaigns, leaflets, booklets, films, posters, or direct mail. . . .*
>
> *Behaviour modification: behaviours are changed through more direct approaches, without assuming that attitudes have an intermediary function, for instance by skills training combined with procedures for providing rewards.*
>
> *Structural modification: contextual factors are changed through legislation, regulation, organisation, and economy. This also refers to changes in the physical environment and to modification and the availability of products.*
>
> (p. 274)

One of the findings from their review is that attitude change is insufficient to drive behaviour change. This reflects common experience. For example, many people know it is right to exercise more and eat less but don't. Simply placing posters on walls, circulating leaflets and posting emails won't achieve much. When combined with training programmes more can be achieved, however, the most powerful impact is achieved by changing the context in which people operate. Changing the context means writing new rules of engagement. Changing context seems to be the most powerful way of changing behaviour, particularly in conjunction with good communication and training.

Imagine a cold room. Staff are seated in chairs and are wearing thick clothing to keep warm. Turn the temperature up enough and eventually people will remove their outer layers. The change in context, in this case the change in temperature, has been enough to change the behaviour of those present. If the context changed in which people worked so too could behaviour be changed. If the context of not wearing safety glasses was dismissal and loss of pension rights, it would be a brave and wealthy person who decided not to bother! Whilst extreme in nature it illustrates the point. If the context was developed that forced behaviour in the required way and was combined with communication and training about the consequence of actions rather than their risk it may help drive a stronger safety culture.

> *. . . when attitude, behaviour, or structural modifications are used in combination, the interconnections and mutual influences taking pace among the personal and contextual factors . . . seem, to produce stronger effects than if one category of preventative measures is used alone.*
>
> (Lund and AarØ 2004, p. 310)

This approach deals with the paradox that Cacciabue (1998) noted in that:

> *The knowledge of a plant operator is principally based on education, training and direct experience. Through basic education the operator knows the physical laws underlying the process but it is only by means of training and experience that he/she becomes acquainted with the plant behaviour in normal and abnormal conditions. It is almost only during training that individuals learn to manage a system in emergency or abnormal operating conditions, while during every day experience the system behaves without incidents. This dichotomy contributes to the creation of a mental bias on the part of the operator who is led to overestimate the plant capabilities to react against anomalies.*
>
> (p. 107)

LEARNING THROUGH SIMULATION

More emphasis is needed on abnormal states and how they should be managed. Procedures are written for the correct process and risk assessments used to determine the likelihood something going wrong and how that might be dealt

with. Lessons need to be learnt from other industries such as aviation. Pilots have to pass a six month test in a simulator in which they are presented with a number of scenarios to test how well they are practiced in the event of a system or mechanical failure. In other words they learn and practice what to do in a crisis and then practice it – regularly.

In the same way, operators should be type rated for the asset they are operating. It is important that this is done for the exact system they should be operating. Where generic training is done the consequences can be catastrophic. It is not enough to educate people at an abstract level. In the Centrica incident at the North Sea Rough Storage facility within the UK continental waters, one of the Coxwains failed to launch a lifeboat because he was the recipient of a refresher course which used as a basis for training a different type of lifeboat starting system than that was actually installed at Rough on the basis the principles if applied were what mattered. In the event, the stress and pressure of the situation meant that when it came to the crunch, he followed the procedures for an electric launch of his craft without effect when he should have prepared himself for a hydraulic starting system which required a different set of requirements. The consequences at the time were all too apparent. There is a need then to provide the appropriate level of training that allows people to deal with a specific situation, such as starting a lifeboat launch, and the level of understanding needed to apply knowledge and experience as to how best to hand a situation. In short, people need to be trained to recognise the signs and how specifically to respond. They need to be part of a wider process of 'risk' evaluation where understanding is and experience are brought together and the ultimate deliverable would be to prepare a highway code where all risks are ranked based on the ultimate consequence and then a set of stop and give way signs set as boundaries of operation. If you get to a stop and hold it directs you to another level of decision, one in which you don't have the ultimate accountability. It also has the benefit for senior managers and directors to see the outcome and then be happy with the risk the business is accepting and then they can reinforce and support any production losses due to the unacceptable levels of risk in continuation of the operator. This supports cultural obligations under the investigation against corporate manslaughter or director responsibilities.

Risk assessments do not effectively teach people how to handle the problem. The plant changes and people just do another risk assessment but it doesn't teach them what they now need to do if the system fails. The speed at which events can escalate mean there is no time other to go into a learnt and practised set of responses that maximise the chance of people surviving the incident.

Decisions must be based on rules, that require escalation at key points to the next level until the right level of knowledge and experience is reached to correctly manage the situation. This means writing an operation manual for each plant, just as there is a manual for flying a plane. That manual is both the procedures for normal and abnormal states.

STOP SIGNS

Whilst the most significant factor in maintaining a safety culture will be the creation of the right context supported by regular simulator training, much can be done to aid understanding. The complex array of lever arch operating procedures designed to accommodate most eventualities does not make for memorable reading and for the worker operating machinery on a daily basis may soon become a vague memory. When expected to understand the risk of one decision over another they may not succeed. When people are asked to assess risk " . . . .they seldom have statistical evidence on hand. In most cases they must rely on inferences based on what they remember hearing or observing about the risk in question." (Slovic, Fischoff, and Lichenstein 1979, p. 183). There are, however, examples where risk is communicated in a much more memorable way. Consider the Highway Code. The signs and symbols within trigger off a series of responses in drivers. The 'Give Way' sign has cars slowing down coming into a junction. The consequences of not giving way are a crash and possible loss of license through charges of reckless driving. The 'Give Way' sign does not contain all the technical information required for the driver in order to give way, such as:

- Look in the mirror
- Slow down
- Change down through the gears
- Indicate

Nor does it provide the additional detail required if conditions are particularly wet, or icy, or foggy. It is left for the driver to know how to respond to these through training and experience and relies on the consequence of not doing so to create the context that drives the required behaviour.

What should also be said is that continually adding more and more signs (procedures) eventually leads to sign blindness and an operator/driver can no longer establish what is important.

What we propose, therefore, is a workers highway code for operating and maintaining an asset. These everyday signs would become the mechanism that governs day to day behaviour to prevent links being established in the chain leading to an incident. Rather than rely on extensive manuals checks and procedures, proper training and development would be supported by a powerful context in which the consequences of action would be clearly understood.

Just as the Highway Code is specific to the road, so too will the Highway Code on hazardous plant need to be specific to that environment and the Highway Code of safety for hospitals needs to be specific to health care.

For the sake of illustration, the highway code of an offshore environment where an operator is responsible for supervising complex mechanical and electrical processes, may include "if you can't gauge it twice – stop". This reflects the fact that almost all systems have at least two gauges or measures indicating the state of a given part of

the system, such as the level in a tank for example. If those two gauges or measures do not correspond, then there is a fault. The fault could be with the gauge, or with the system, but somewhere there is a fault and therefore appropriate steps need to be taken to validate where the problem rests and then manage accordingly. The consequence of not stopping should be sufficient to drive the right behaviour, e.g. points on the licence, loss of earnings and if necessary loss of employment.

As another example the highway code for placing maintenance inhibits on a control system input maybe "a maximum of 1 maintenance inhibits can be in operation at any given time". It removes the operator's view that the design of maintenance inhibits on the system and his authority of application allows for endless application as long as a risk assessment has been completed. It is a leap of faith to believe an operator can clearly understand the significance of the first inhibit whilst managing its associated temporary mitigation control and then go on to understand the second both in isolation, system interdependence to the first, two separate temporary control structures in place and whilst managing his 'normal operation'. It is with pride operators are attempting to maximize plant uptime but care must be taken to prevent undue pressure and make that pride defeat logic. The right consequences for unsafe practice could overcome this.

There needs to be an efficient and effective process of escalation. This is not about risk assessments and micro level procedures, instead it is a focus on the key areas where people can and cannot make decisions. These decision gateways either allow people to pass onto the next decision or indicate where someone cannot pass. It is akin to 'financial budgets' in that a manager can spend up to a specific amount without requiring authorisation, after which they need permission. This means determining acceptable levels of risk in advance and the critical points for decisions. Each escalation at the decision gateway is the equivalent of taking a major link out of the chain. This is practiced in simulation exercises.

The context is key to the effectiveness of implementing the highway code. There be real and relevant consequences to failing to operate by the highway code of safety in industrial processes. It starts by legitimizing acceptability of *not knowing*. The illusion of competence created by the supposed value of years of experience cannot be given credence beyond the true level of competence the individual has. Some signs should have instant, dramatic and significant consequences to drive home the importance of obeying that sign. These might be considered 'Red Rules' and a failure to comply is an instant dismissal. There is the apocryphal account of the maintenance operator replacing stair treads. The procedure stated take one stair tread out at a time to replace them. Decades of experience had 'taught' the operator that it was easier to take two at a time. The 'red rule' would be only one stair tread at a time. This would be a red rule because the gap created by removing two treads was large enough for the operator to fall through. The consequence of falling through the gap on certain stairs is death, as proven by the operator. The processes and procedures were meaningless and ineffective at preventing the death of the operator. Had he been at risk of losing his job for removing two treads, the benefit would not have outweighed the consequence and instead he may have been looking forward to a well earned retirement.

'LINKS IN THE CHAIN'

The 'links in the chain' model begins with a fundamental shift in approach to safety from minimizing risk to the lowest level possible to helping people understand that without their activity myriad events will eventually link together to form catastrophes in unknown and unanticipated ways. Each individual has a responsibility to recognise that every single action or inaction either puts another link in the chain to failure or takes one out. Enough people taking enough links out will make the operation of a facility safer.

A plant is designed at the macro level based on multi disciplinary knowledge looking at the interactions between all the decisions taken. In a COMAH or safety case there is a multi disciplinary knowledge looking at the interactions between all the different elements and determining it is safe to operate under a given set of rules and conditions. It won't and cannot look at every possibility. Codes and standards set the boundaries for safe operation. Communication, accreditation through simulation (training and education) and the right context will drive the right behaviour. However we need to start by fundamentally changing the way people think:

From	'safe'	to	'less risky'
From	'risk'	to	'consequence'
From	'process and procedures'	to	'a highway code'
From	'competence'	to	'accreditation through simulation'

We need to help operators understand that their each and every action and inaction either links the actions and inactions of others together to lead to an incident, or they can take the decision to remove the link.

REFERENCES

Cacciabue, P.C. (1998) Modelling and simulation of human behaviour for safety analysis and control of complex systems *Safety Science*, Vol. 28, No. 2, pp. 97–110.

Henderson, D. (1991) Ocular trauma: one in the eye for safety glasses *Archive Emergency Medicine*, Vol. 8, No. 3, pp. 201–204.

Irvine, D. and Wilson, J. (1994) Outdoor Management Development – Reality or illusion *The Journal of Management Development*, Vol. 13, No. 5, pp. 25–37.

Kontogiannis, T. (1998) User strategies in recovering from errors in man-machine systems *Safety Science*, Vol. 32, pp. 49–68.

Le Coze, J. (2005) Are organizations too complex to be integrated into technical risk assessment and current safety auditing? *Safety Science*, Vol. 43, pp. 613–638.

Lund, J. & AarØ, L.E. (2004) Accident prevention. Presentation of a model placing emphasis on human, structural and cultural factors *Safety Science*, Vol. 42, pp. 271–324 p. 693.

Reason, J. (2000) Human error: models and management *BMJ*, Vol. 320, pp. 768–770.

Slovic, P., Fischoff, B & Lichenstein, S. (1979) Facts and Fears: Understanding perceived risk *Proceedings of an international symposium* Oct 8–9 General Motors Research Laboratories, Warren Michigan, pp. 181–185.

Thornton, H. (2003) Patients' understanding of risk *BMJ*, Vol. 327, pp. 693–694 (27 September).