HOW TO REDUCE HUMAN FAILURE

Considering human factors could be the best way to catch an error before it happens

JANETTE EDMONDS
DIRECTOR AND PRINCIPAL CONSULTANT ERGONOMIST, THE KEIL CENTRE

THERE is a recurring number that despite magnificent developments in technical safety doesn't seem to go away. That number is 80, and it relates to the percentage of incidents that in some way has been contributed to by a human. It is a recurring average across industry and in different settings. Looking on the bright side, it means that there is huge scope to make a significant improvement.

So how can we reduce the rate at which people contribute to incidents? The first step is to recognise that human failure is not random, but systematically linked to the tasks that people perform, the equipment they use, and the characteristics of the work environment. By understanding these elements it is possible to reduce the potential for errors to occur in the first instance, or at least to pre-empt them so that when they do occur, they can be safeguarded against.

This article provides an overview of human failure, the factors that contribute to it and the process by which the risks can be reduced.

WHAT IS HUMAN FAILURE?

There are a number of different ways of describing human failure, and I've used that term on purpose, because failures can include human errors and violations (also described as non-compliances). In simple terms in the context of safety, human errors are unintentional unsafe behaviours and violations are intentional unsafe behaviours.

For any incident it is possible that there will be both errors and violations. Take the example of the Formosa plant explosion in Illinois in 2005 (investigated by the US Chemical Safety Board). An explosion occurred at the polyvinyl chloride (PVC) production unit, killing five workers and seriously injuring two others. The incident occurred during the cleaning of Reactor 306 whilst Reactor 310 was midway through a PVC reaction containing highly explosive chemicals under heat and pressure. During the cleaning process, the operator was required to empty the cleaning fluid out of Reactor 306 by opening the bottom valve to drain. The operator walked from the top floor of the reactor building to the lower floor, and turned right instead of left at the bottom of the stairwell. He then opened the bottom valve on the working reactor (310) instead. This reactor did not drain, as a safety interlock was installed to prevent the bottom valve being opened while under pressure. However, the operator then bypassed the interlock by attaching the emergency air hose, and the reactor contents were released. Rather than evacuate immediately, the supervisor and operators tried to deal with the ongoing spillage and five were killed when it ignited. During the investigation, it was revealed that similar errors had occurred in the past and that there had been a failure to properly assess the risk of human error in the design. The emergency and evacuation procedures and training were also identified as inadequate.

In this example, the first human failure was that the operator went to the wrong reactor in order to drain it. This is an example of an *error* (he didn't mean to go to the wrong reactor). He then used the emergency air to bypass the safety interlock on the bottom valve. This is an example of a *violation* (he intentionally did something he shouldn't). Finally, the supervisor and the other operators tried to deal with a situation which was uncontrollable. It is debatable whether this is an error or a violation, but given that the emergency procedures and training were identified as inadequate, it is likely that this was an error.

Human failures are not just restricted to the frontline of the operation. They can occur at all levels of an organisation and can directly or indirectly contribute to a major incident. For example, a management decision to reduce staffing numbers without assessing the impact on the operation, or a maintenance team failing to correctly calibrate the instruments for a safety critical trip function. These would be referred to as *latent* failures, rather than *active* failures at the frontline.

WHAT FACTORS CONTRIBUTE TO HUMAN FAILURE?

What has been described so far is the actual failure itself – the 'what' – what has happened, or what could happen. But there are factors that make the failure more likely to occur. There are different terms that are used to describe these factors, but one of these terms is performance shaping factors (PSFs). PSFs are aspects of the work context, such as the examples in Table 1.

Many of these factors are relevant to violations as well as errors. These factors are sometimes referred to as *antecedents* (ie 'triggers' for the intentional behaviour) when analysing violations.

The next example, relating to the Buncefield accident, also in 2005, and investigated by the Health and Safety Executive, demonstrates multiple human factors failings at all levels in the organisation.

A series of explosions occurred at the Hertfordshire oil storage facility in England. Thankfully no-one was killed, but 43 people were injured, hundreds of people had to be evacuated, and there was significant blast damage in the vicinity. It was acknowledged that if the accident had occurred during normal office hours, the numbers injured and killed could have been significantly worse.

Storage tank 912 was being filled with petrol. The tank level was routinely monitored using a level gauge and had an independent high-level trip to shut off the inflow above a specific set point. On the morning of the accident, the manual level gauge was stuck, tank 912 overfilled, and the high-level trip did not operate. The petrol escaped undetected through vents in the top of the tank, formed a vapour cloud, and later ignited and exploded. The ensuing fires lasted for five days.

The level gauge had stuck intermittently over the previous months and the trip switch was not locked in position to enable the check lever to work. The bund failed, allowing petrol to overflow, and the drainage system also failed, later causing firefighting foam to enter the groundwater supplies. Both of these containment systems were inadequately designed and maintained.

TABLE 1: EXAMPLES OF PERFORMANCE SHAPING FACTORS

CATEGORY OF PSF	EXAMPLES
The task	A highly complex task or high workload causing someone to rush to finish a job
Communications	Poor handwriting; inaccurate use of language; heavy accent
Procedures & documentation	Ambiguous wording or the procedure not matching the task as it is performed; the piping and instrumentation diagram (P&ID) being incorrect
Environment	High background noise; poor lighting; vibration affecting performance
Training & experience	Lack of experience or recent training
Human-machine interaction	A flood of alarms or a poorly laid out control screen
Personal	A recent bereavement; being fatigued from excessive shiftwork
Social & team	Personality clash; poor inter-team coordination

HUMAN FAILURES CAN ALSO BE PROACTIVELY MANAGED THROUGH IMPLEMENTING A STRUCTURED RISK ASSESSMENT PROCESS

The investigation also revealed deficient management safety checks. The operators were given insufficient pipeline information to properly manage the storage of incoming fuel and to identify unfolding abnormalities and emergency situations. The control room was poorly designed and laid out. Production was also found to be prioritised over safety, and throughput had been steadily increasing, adding to the pressure and complexity of the operators' tasks. Chronic staff shortages and poor shift and work planning combined to cause excessive fatigue. The procedures were inadequate, especially in relation to ullage management, hazards (such as overfilling tanks), and control room activities. Training was unstructured, with little instruction on upsets and emergencies, and the competence management system was not well developed. In addition, the shift handover was unstructured and informal. There were clearly multiple human factors failures that contributed to the accident.

HOW CAN WE REDUCE HUMAN FAILURE?

Human failures are often identified reactively through incident investigations and this is one mechanism by which to reduce the potential for a recurrence of the event. However, human failures can also be proactively managed through implementing a structured risk assessment process. The core methods used are referred to as human reliability assessment (HRA) and there are qualitative and quantitative methods that can be used. In my opinion, the qualitative methods elicit the required information in the majority of cases and avoid being distracted by probabilities which can erroneously be taken as absolute rather than relative predictions of human failure.

SAFETY CRITICAL TASK ANALYSIS

Implementing a programme of HRA across a site or a system would take considerable time, effort and investment. This is the key reason why a risk-based approach is typically used. The approach is known as safety critical task analysis (SCTA), and the Energy Institute outlines a seven-step process, as shown in Figure 1.

Effectively, steps 1 and 2 are used to identify and prioritise the most safety critical tasks so that attention can be given to those first. A safety critical task is one which, if it is not performed or performed incorrectly, could contribute to a

major accident or impair a safety critical element. Steps 3–6 represent the basic process of HRA.

SAFETY CRITICAL TASK IDENTIFICATION

Steps 1 and 2 may be referred to as safety critical task identification and the output is often presented as a list of all the tasks on site, including operational, maintenance and emergency-related tasks, ranked in order of safety criticality: high, medium and low. There are different methods for doing this, including simple methods, such as rank ordering all procedures on site using a basic human risk matrix (see Energy Institute, *Guidance on HF Safety Critical Task Analysis*, *bit.ly/29ib07u*). In my experience, simple methods have their drawbacks, such as excluding important tasks which are not the subject of procedures, procedures being out of date or in a poor state of health. They can sometimes over-estimate the safety criticality of tasks.

HUMAN FAILURE CONTRIBUTES TO 80% OF ACCIDENTS, WHICH MEANS THAT THERE ARE GREAT SAFETY IMPROVEMENTS TO BE GAINED

The longest-standing method is the subject of the HSE guidance document *Human Factors Assessment of Safety Critical Tasks* (bit.ly/297QnOC). This was developed for the offshore oil and gas industry but has been used with minor modification for other applications. For each task identified, a set of diagnostic questions are used to rate the task from low to high priority, adopting a specific safety criticality score. There are different diagnostic questions for production operations and well operations. These have been developed on the basis of the hazards involved, the key concerns relating to major accidents, how human interaction can affect the realisation of an accident, and weaknesses in protection systems which can make the system vulnerable. In my opinion, this is an excellent method and provides a structured, comprehensive and effective process for understanding the safety criticality of tasks.

Other methods have been emerging over recent years involving the incorporation of human factors within established safety assessment methods. An example is human factors within bowtie analysis. More often than not, human factors has been perceived as an add on to these analyses, even to the extent where a single threat or fault tree branch is added with the label of human error. It is recognised within the human factors community that this approach is symptomatic of failing to properly integrate human factors into the safety analysis process. There needs to be more intrinsic and pervasive questions within the analysis, such as '*for this threat barrier, how can it be undermined by human interaction?*'; '*how can the human initiate a threat?*'; '*how can the human fail to mitigate or recover from the top event?*' The Chartered Institute of Ergonomics and Human Factors (CIEHF) plans to publish a white paper this year on the topic of *Human Factors in Barrier Thinking* to progress the integration of human factors within safety analyses. Despite the developments in this area, there will still be a need to continue the rest of the process to understand safety critical tasks in more detail and to reduce their risk through structured HRA.

FIGURE 1: SEVEN STEPS OF SCTA

1. IDENTIFY MAIN HAZARDS (TYPICALLY FROM SAFETY ASSESSMENTS / REPORTS)
2. IDENTIFY CRITICAL TASKS (TO PRIORITISE THE EFFORT)
3. UNDERSTAND THE TASKS
4. REPRESENT CRITICAL TASKS
5. IDENTIFY HUMAN FAILURES AND PSFS
6. DETERMINE SAFETY MEASURES TO CONTROL HUMAN FAILURES
7. REVIEW EFFECTIVENESS OF PROCESS

HUMAN RELIABILITY ASSESSMENT

Systematic human error and reduction prediction approach (SHERPA) is one of the most well-known HRA techniques and is typically undertaken in a workshop setting with operations, safety and engineering experts in attendance. The starting point is to understand tasks in more detail (steps 3 and 4).

For each task, credible errors are identified using a set of guide words, such as "action error: too much/too little", "right operation/wrong object". These are translated into error statements, such as "failing to isolate the valve on the process train being prepared for maintenance" (action error: right operation/wrong object).

PSFs will be systematically reviewed to understand how the error could be made more likely, such as no tag identities on the valves (human machine interaction issue), or the task is performed at 03:00 (fatigue issue).

The consequences of the error are identified. In this case, the consequence may be a loss of containment during maintenance, so this is an example of a *latent* error where the consequences are not realised at the same time (or space) as when the error occurred.

The means by which the error would be recovered are identified. This is not the risk control measure, rather it is 'how

would someone know that they have done something wrong and then be able to rectify it'?

Existing or planned risk control measures are reviewed to identify how the error (or violation) might be prevented in the first place, detected and/or mitigated. Where there are gaps in the control of the error, additional control measures are recommended. The recommendations follow a hierarchy of control, with engineered solutions being the preferred option, followed by human controls (such as supervision, procedures, training and checks). The assessment of risk pre and/or post risk control may be included within the HRA process.

In my experience, this process is extremely effective at identifying potential human failures and has been a real eye-opener for design teams and operational sites alike. For example, during one analysis, the HRA process was undertaken for a chemical top tier Control of Major Accident Hazards (COMAH) site for the task of charging a vessel with specific materials. An error was identified for a very simple task that had never been considered before and had an uncontrolled risk which could have led to a catastrophic event. The site acted by immediately stopping this specific charging event until a risk control measure could be engineered.

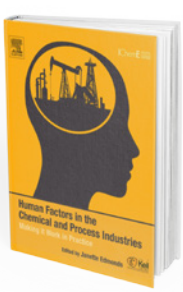
It is important to recognise that SCTA and HRA are quite different from other safety analyses but absolutely complementary to them. It is also fair to say that many safety analyses do not adequately assess the human contribution and in particular how human behaviour can undermine risk controls already in place. Even a safety interlock is only as good as the person maintaining it.

SHOULD WE ONLY FOCUS ON FAILURE?

There is a tendency to over-focus on human failure without properly acknowledging the success that comes from human involvement within the work system. Human performance variability is essential to making things work in practice, and can save a critical situation from becoming a disaster (take for example the aircraft landing on the Hudson River in 2009 despite the odds against success). So there is a need to understand, that if on most days most things go right, why this is the case, as well as why they sometimes (typically rarely) go wrong. The answer is often that people are either working around problems or that those systems concerned are in fact well-designed for people. By finding out what people are working around, it is possible to improve system resilience. That means not just investigating incidents and work systems comprehensively but learning from operational experience. The role of human factors is to understand how humans can contribute to optimal performance of the system, assure safe human performance, and thereby enable a higher safety standard.

CONCLUSION AND SUMMARY REMARKS

Human failure contributes to 80% of accidents which means that there are great safety improvements to be gained. There are different types of human failure but a simple distinction is used to understand the difference between *errors* (unintentional unsafe behaviours) and *violations* (intentional unsafe behaviours). There are factors that make failure more likely, both errors and violations, and these are often referred to as performance shaping factors or antecedents in the case of violations. Human failures can occur at any level within an organisation, not just on the front line, and these need to be considered both reactively in incident investigation but also in a proactive structured risk assessment process. ■



The consultant team at the Keil Centre has written a book for the chemical and process industries, providing guidance and advice for integrating human factors in a practical way. The book is due for publication by Elsevier in October 2016.

Disclaimer: This article is provided for guidance alone. Expert engineering advice should be sought before application.

Human Factors in Health and Safety

This modular training programme examines the core human factors issues in the process industries and how to manage them effectively to improve safety and business performance.

www.icheme.org/humanfactors

the Keil centre
chartered psychologists & ergonomists

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE