How do we reduce the number of accidents involving human factors?

Prepared on behalf of the IRSE International Technical Committee by Rod Muttram

"*To err is human, to forgive divine*" – from "An Essay on Criticism" by Alexander Pope (1688 – 1744).

Currently, human error is undeniably at least a contributory factor in the causation of most accidents and incidents. Human beings are prone to making errors for a wide range of circumstances, some of them beyond their reasonable control. Yet humans are often held responsible for the consequences of those errors regardless of the contribution made by the system and the environment within which they were working. Historically forgiveness has often been sadly lacking, whatever the situation. A good example would be the prosecution and conviction for manslaughter of the driver of the train which passed a red signal leading to the Purley crash in the UK in 1989. His train struck the rear of a train which was crossing onto the fast line from the slow following a scheduled station stop; with the first six coaches of his train derailing and plunging down an embankment, killing 5 and injuring 88. Despite a guilty plea his sentence was subsequently reduced and then overturned as unsafe in 2007. This followed the analysis of human interaction with the Automatic Warning System (AWS) exposed at the public inquiry into the Southall collision (see below); and the recognition that 'something about the infrastructure of this particular junction was causing mistakes to be made ' coming from new analysis of multi-SPAD signals showing that there had been four previous signals passed at danger (SPAD) at this location in the five years before the crash, far above the 'all signal average'.

So, whilst it remains reasonable for employers, regulators and the general public to expect those employed in delivering transport to be diligent in their duties, that diligence must be judged in the light of all of the circumstances that contribute to any failure. More importantly those designing systems and processes (including the design processes to produce the systems) need to understand human performance and take it into account to minimise potential failure/error rates and mitigate any consequences. With the excellent safety performance currently being delivered by many railways it is vital that we do not become complacent and miss new risks emerging from a combination of incremental changes.

What are Human Factors?

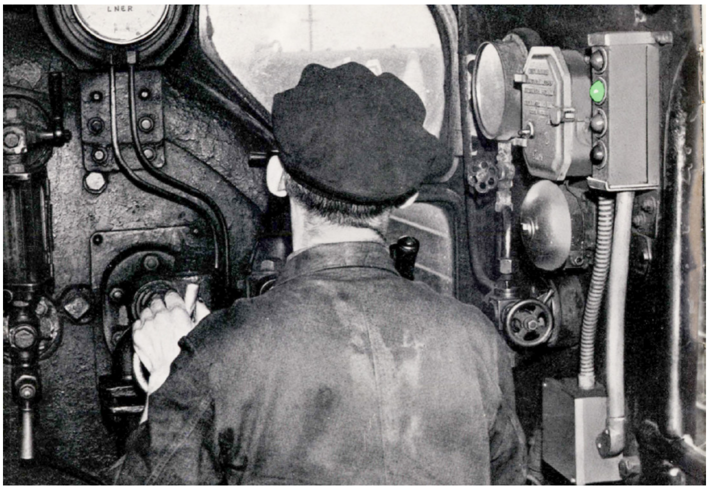
The performance of all systems is dependent on people, processes, equipment/tools and the interaction between them. To date, even automatic systems have all been designed by humans who may leave unintentional embedded errors. 'Human factors' is a broad term for the analysis and optimisation of human performance in the workplace. It should consider the working environment, interfaces and processes from a human-centred viewpoint, by looking at the whole system and its influence on the way people make decisions and interact with the other elements and each other.

Another term used is 'ergonomics', a simple definition of which is 'making life simpler and safer by taking account of human characteristics when designing things '. There are three branches of ergonomics corresponding to the elements mentioned above:

- Cognitive ergonomics (concerning people's perception, reasoning, memory, motor response etc.).
- Organisational ergonomics (the impact of organisation structure, policies, processes, culture, etc.).
- Physical ergonomics (how people interact with equipment and tools including things like work layout, the design of symbology, required reach, strength etc.).

Human factors may be considered a generic term for all of these areas. Whilst on a railway or metro the roles of train drivers, signallers/train dispatchers, and other front line staff tend to be the most affected by human factors, all railway staff are impacted to some degree.

Human factors is a relatively new formal discipline in the railway industry. In the UK, whilst some specific studies had gone on earlier, the first dedicated human factors team was set up within Railtrack's Safety and Standards Directorate during the 1990s and was the origin of the current team within the RSSB (Rail Safety and Standards Board). Most other countries started to think seriously about such matters at around that time, whilst others have yet to begin formal consideration. Of course, many past 'custom and practice' ways of doing things (for example staff selection tests for particular roles based on certain aptitudes) were founded on human factors principles but often without much discipline or rigour. Concern is often raised about the potential for errors when workloads are high, but rarely when they are too low which can lead to boredom and distraction and thus also have a detrimental impact on failure free performance.



The quest to make life easier for the human in the loop – in this case the driver of an LNE steam locomotive in the 1940s in this Westinghouse publicity shot – is a long running story. *Photo Westinghouse archive.*

Examples

A few examples are now given to illustrate the different facets of human factors, and how they sometimes combine:

Cognitive Issues

The example given above (Purley) and a number of other accidents where the British Rail AWS system has been implicated are good examples of cognitive issues. The original AWS technology dated from the early 1950's (and had its origins in even earlier systems of 1906 and 1930) and was based on a magnetic interface between track and train. It was designed to alert drivers approaching a two-aspect distant signal as to whether braking needed to be initiated. It was not even originally fitted at two-aspect stop signals. It only had two states 'clear' and 'warning' (or more accurately 'not clear'). For 'clear' a bell or chime was rung and an indicator remained black; no action was needed by the driver. If a warning was received a buzzer would sound and the brakes would be automatically applied unless a cancel button was pressed within a few seconds (nominally 2.75 seconds). When the warning was cancelled a yellow and black 'sunflower' indicator reminded the driver that the last signal was 'not clear' with the expectation that the train would be controlled appropriately. The indicator was reset the next time a clear signal is passed.

AWS continues to be better than no protection at all but the application of a system with only two states in later three- and four-aspect signalling territory potentially leads to 'systematic automatic' behaviour with routine cancellation of the warning. The warning is the same regardless of whether the signal is double yellow (preliminary caution), yellow (caution - prepare to stop) or red (stop). In heavy traffic the driver may be running with repeated double yellow or yellow aspects, rarely seeing green and repeatedly cancelling the warning and driving on. If the driver then approaches a red signal it is all too easy with concentration not at 100% (perhaps due to a distraction) to cancel the warning in an 'automatic' way and drive on into a dangerous situation. The later Train Protection and Warning System (TPWS) supplemented AWS by adding a train stop and/or a speed trap at high risk locations.

Who among us can genuinely say that we have not experienced problems caused by learned behaviour leading to automatic responses? In the UK and Japan, road traffic drives on the left side of the road. The steering wheel is on the right of the vehicle and the direction indicator stalk is normally on the left side of the steering column to conform with continental Europe and America where traffic drives on the right side of the road with the steering wheel on the left. The convention in UK vehicles until circa 1970 was to have the indicator stalk on the right-hand side of the wheel (the outside) and indeed some Japanese cars still have this arrangement. Drivers of older cars and some imported Japanese models can get confused if faced with a hire or loaned vehicle and will likely operate the windscreen wipers instead of the indicators. Rarely does this lead to an accident but potentially dangerous situations can arise. It is likely most people reading this will have had similar experiences. So why do people still think it is reasonable to design systems that require high levels of operator accuracy to two or more different conventions?

Organisational issues

AWS also provides a good example of organisational ergonomics and of procedural issues associated with human factors. On 19 September 1997 a high-speed train (HST) heading towards London collided with a freight train crossing a ladder junction at Southall near London. The HST was being driven with the AWS isolated due to a fault. It was also fitted with the Alstom/ACEC TBL1 automatic train protection (ATP) system as part of a pilot trial, but that was not switched on. The train's journey had originated in Swansea, South Wales, where a triangle existed that could also have turned the train to put the other cab, in which the AWS was working, into the leading position. The train had passed double yellow and single yellow signals at 200 km/h and had only started to brake (much too late) at the red signal. The driver of the HST (who survived) was apparently packing his bag ready for arrival at the terminus and had not observed the yellow signals, only braking just before the red signal. Seven passengers were killed and many more injured. The circumstances of the Southall collision were investigated by a wide-ranging public inquiry chaired by Professor John Uff CBE FREng QC. Amongst many factors considered, the situation of running a train with no active protection system was a major consideration.

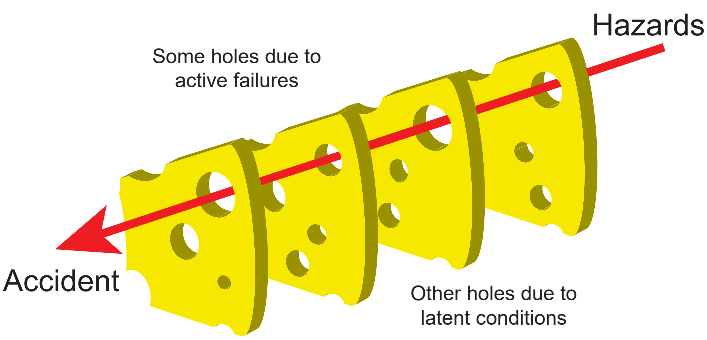
The British Rail rule book still current at the time allowed such a circumstance to happen. AWS was considered a 'driver's aid' and it was the driver's job to safely control the train at all times. The only restriction required if AWS was unavailable was to impose a speed limit in foggy conditions if signal sighting was impaired. It transpired that no effective rules existed as to what should happen if any piece of on-train safety critical or safety related equipment failed. Evidence to the inquiry by human factors experts made clear the folly of this situation for AWS. The existence of a system which normally provided audible and visual warning of the approach to, and status of, signals would inevitably lead to drivers relying on that system to some degree. Resulting from the inquiry, a new Railway Group Standard was developed governing the management of on-train safety equipment. For AWS, if the fault could not be rectified or the train turned, it required that the train stop at the next suitable station and de-train its passengers, then to proceed to a repair depot at either at reduced speed, or with a second trained person in the driving cab.

Physical issues

The third dimension of physical ergonomics yields numerous examples. A badly designed handle may mean loss of grip with failure to operate it at a crucial moment. Trying to lift something that is heavy and awkwardly shaped without the appropriate tools or fixtures may lead to personal injury. There are many more subtle reasons for equipment being badly designed in terms of the human interface; the use of similar symbols with different meanings or small symbols which are hard to read in an emergency or critical commands being buried within a menu of other commands are examples, especially if a person is under pressure (see the description of the accident at Bad Aibling in Germany below).

Multiple causes

Professor James Reason's 'Swiss cheese' model puts forward the thesis that accidents happen when gaps in our protective 'safety barriers' align with several failings happening simultaneously akin to the holes in several random slices of Swiss cheese occasionally aligning so that a hole appears right through. This is often the case with human factors where combinations of different failings come together and lead to an accident. Two examples (one



Professor James Reason's 'Swiss cheese' model has appeared many times in IRSE News, but is one of the clearest ways of demonstrating the way that accidents can happen when gaps in our safety defence occur.

Modern control centres are often complex, high-intensity work environments. Do we always consider the human factors involved in operating such critical systems? *Photo Network Rail.*

railway and one non-railway) are described below; the ergonomic issues are not specifically identified by type; readers are asked to consider the situations and the subsequent events from a human factors perspective.

The author personally recalls the non-railway example which concerned a workplace fatality. It happened in a factory which made hard rubber and thermoplastic mouldings, mostly for use in the manufacture of vehicle batteries. The old 'black rubber' car battery cases were made from around 70% ground coal, bound together with rubber, which along with vulcanising sulphur, catalysts and other minor ingredients, were all mixed up, several tons at a time, in a large machine called a Bridge Banbury mixer. This was heavy engineering with large smear mixing rotors driven by 120 hp motors through reduction gearboxes, and drop doors (outlets) on the bottom of the machines weighing around a ton activated by substantial hydraulic motors. A third machine had been added between the two original machines to increase capacity.

This addition resulted in two consequences relevant to the accident: The machines were numbered 1, 3, 2 left to right looking from the front, and the new machine in the centre had a short conveyor beneath it to take material to the next stage of the process, a two-roll mill (rather like a giant mangle), which due to the constraints of the original installation needed to be somewhat offset from the centre of the mixer. On the night of the accident the drop door of machine number 2 (the right-hand machine) suffered a failure and was being worked on by the maintenance team. During the same period the conveyor under machine 3 (in the centre) suffered a blockage. Despite clear instructions and training never to do so, the mill operator stopped the mill, climbed up on top of it, crawled up the conveyor duct and started to clear the blocked material by hand: perhaps trying to be helpful or perhaps because the factory operated a piece work system with operators paid on the output achieved.

The maintenance team believed they had rectified the fault and asked their electrician, who was a new employee, to go and perform a test operation of number 2 drop door. With hindsight, outcome was predictable. The electrician went to the control station, counted '1', '2' from the left and operated the drop door on the centre machine (which was, in fact, number 3). The mill operator in the conveyor duct under mixer 3 was crushed, dying almost instantly, a terrible and wholly avoidable accident, which had a big impact on everyone involved. The aftermath required many procedural improvements, the addition of guards, several different interlocks installed and the machines re-numbered in a logical sequence. With hindsight, most of the factors leading to the accident were very obvious; taken in isolation each seemed to present a very low risk, but when they all came together a man lost his life in a truly horrible way. The author learned a great deal and this was one of the events that fostered his interest in improving all aspects of safety.

The railway example is the collision at Bad Aibling in Germany on 9 February 2016. Here thanks must go to Peter Van der Mark, a former train driver and frequent writer on the importance of looking at things from a human perspective, also to the German speaking members of the ITC, particularly Jens Schulz. At the time of writing only a preliminary inquiry report had been published and nothing said here is intended to pre-empt or contradict the final report and recommendations of the official inquiry; further facts may emerge; our intent is only to highlight the apparent human factors issues.

At 6:47 in the morning, a 174 tonne ET325 six-car and a 111 tonne ET355 three-car train (modern EMU sets built to crash norm DIN/EN 15227) collided head-on with an impact speed of around 150 km/h (90 mph) near Bad Aibling Kurpark halt on the 37 km single track overhead electrified line between Holzkirchen and Rosenheim in Bavaria, Germany. There were initially 11 fatalities, and 85 injured (24 severely with one subsequently dying).

The line has five passing loops at stations, located approximately 5 kilometres apart with the section Heufeld via Bad Aibling to Kolbermoor being controlled by the signaller at Bad Aibling using a 1970's SpDrS60 push-button relay NX (entry/exit) panel. The remote control of Kolbermoor appears to have involved some compromises in the normal technical controls/indications available to the signaller at Bad Aibling and these seem to have been a factor in what happened. The line can be busy in times of disruption on the electrified double-track (Innsbrück – Kufstein, Austria) – Rosenheim – Munich main line as it is the primary diversionary route. Freight services regularly use the line. The impression is a line having periods of intense activity interposed with some very quiet periods. It runs beside the river Mangfall and in places dense vegetation restricts visibility. The line-speed is generally 120 km/h but the collision site was on a curve with a 100 km/h permanent speed restriction (PSR).

As timetabled the two services were due to cross at Kolbermoor station. The westbound service M79506 from Rosenheim to Holzkirchen entered the Kolbermoor station loop on-time and was booked to wait 5 minutes for the opposite service to arrive, but it left on time on a proceed aspect without the eastbound service arriving. The eastbound service M79505, from Munich via Holzkirchen to Rosenheim was due into Kolbermoor from Bad Aibling, but was running 4 minutes late. The signaller stated that when he tried to set the route from Bad Aibling to Kolbermoor the signalling did not accept his input for M79505. His reaction was to consider this a 'phantomstörung', a spurious fault, and he then used the Zs-1 signal facility to override the stop aspect at Bad Aibling and repeated the error using the same facility at Zentral Blocksignal 313 between Bad Aibling and Kolbermoor, presumably to speed the train towards the booked meeting at Kolbermoor. Maybe he expected the on-time westbound service M79506 to wait for the booked crossing despite having previously (and perhaps automatically) given it clearance to Bad Aibling (and thus a proceed aspect) which had prevented him from clearing the signal for M79505. The Zs-1 'Ersatzsignal' as defined in the German railway signalling handbook, has two variants, the first is a small triangle of steady white lights under the main signal, the second a single flashing white; both are meant to allow a train to pass a failed main signal without the need for oral contact between signaller and driver. The first type is used within Bad Aibling area. Having already passed its signal, the driver of M79506 was unaware of any issue with the route ahead. The driver on the delayed M79505 at Bad Aibling adhered to regulations on a Zs-1 aspect at Bad Aibling by passing the PZB ATP magnet at the signal at 40 km/h (25 mph) until clear of the single-line turnout and then accelerated to 100 km/h (60 mph) in accordance with the rules. The signaller eventually realised his first pair of linked mistakes and attempted an emergency stop message on the GSM-R train radio. In his stressed confusion he made another mistake and used a wrong call destination field on his GSM-R computer screen sending the emergency message to station staff along the line. This mistake was quickly noticed resulting in a second successful call, but by then it was too late, the collision had become unavoidable.

There are a number of ergonomics issues here regarding the design and use of the Zs-1 within the overall signalling and operating system:

The rules for the use of the Zs-1 Ersatzsignal require that the line ahead is checked clear and then the aspect may only be used when the associated main signal cannot show a proceed aspect because of a known fault or the need for a 'special move' protected by the relevant rules. Clearly that was not case on the day of the accident.

The use of Zs-1 is logged on an automatic counter and the signalling book has to be filled with the logged number and an explanation as to why the Zs-1 signal was used. Following the accident, various media reports suggested that Zs-1 signals were being used outside of the rules and that other accidents had resulted.

So one must ask:

a) Why was it so easy to use the Zs-1 aspect? The decision was taken by a signaller on his own, without further recourse to either another person, a well-structured checklist or any other equipment confirming the validity of the decision in terms of train safety. A single (if repeated) human error (perhaps consequent on an earlier automatic and unconscious action) produced a catastrophic situation. Pressures on system capacity are leading to more and more pressure to install secondary override systems to keep trains moving. These might compromise the fail-safe principles the industry has refined over many decades and great care must be taken in returning to reliance on human decisions, however much they are wrapped up in some form of technical implementation.

b) Why was it so easy to overlook section occupation? Like many other relay signalling installations, the Siemens SpDrS60 panel shows the set route as a string of yellow lights on the track panel diagram. If a track circuit becomes occupied the string of yellow lights changes to a single red occupied section light. A long single track section between stations, may be overlooked as showing occupied. The illustration of the SpDrS60 panel in the interim report indicates that track circuit occupation may not provide reliable perception by a distracted operator. Checks on the Internet do not materially change that impression.

c) Is it really safe to allow a service departing on a Zs-1 aspect to travel at line speed when the Zs-1 aspect is used because of degraded/faulty signalling? Even if the rules prescribe several types of signaller checks that the track ahead of the signal is clear, there is evidence from at least three accidents indicating uncertainty as to whether those checks are always effective, particularly if one person controls a long section of line. 'Proceed on sight' at a reduced speed would seem more prudent, but introduces more delay. Any such genuine equipment failure might be better protected by the use of a 'sweep train' to remove any uncertainty.

d) How effectively were the signalling records used as part of the safety management system? The checking of the signalling book, the signalling fault book and the Zs-1 signal occurrence counter figures by supervisors does not appear to have been either frequent or thorough, nor do lessons learned seem to have been followed through. That could be interpreted as either a lack of safety leadership or, worse, a tacit agreement with misuse.

e) Why was the wrong radio screen destination field used to distribute the emergency message? It is surprising to find that the GSM-R human machine interface design was such that the emergency stop message to train drivers, which is almost always used under stressed conditions, required the clicking of the correct button amidst an array of message destination fields. It is likely that the collision could have been avoided had the first message been received in the cabs. In an emergency situation absolute clarity is required both where the message is initiated and where it is received.

f) Is it really wise to provide a Zs-1 signal at a main signal that provides the entry protection to a single line section, at least without some structured procedure or system to mitigate the risk of an oncoming train?

There were also potential low workload issues, with reports indicating that the signaller had been playing a game on his smartphone immediately prior to his original error. This distraction might have contributed to the earlier clearing of the route for M79506 from Kolbermoor without subsequently being conscious of that action. One wonders how well the signaller had been trained and supported to cope with varying workloads though the shift.

It seems there was no single cause but again, the 'holes in the Swiss cheese' aligned.

Maintenance

Human factors issues are not constrained to design, construction and operation, but can impact on maintenance. When developing enhanced safety rules associated with maintenance work that extend the total time taken, how advantageous might these be viewed by a work gang on a cold winter night at 2am in the pouring rain?

Some examples of human factors related issues in maintenance:

- Work being undertaken by staff without the necessary competence (or licence) to avoid delay – this has many risks.
- Wrong interpretation of status information provided from the signalling system (e.g. track circuit information on train whereabouts).
- Unintentional use of incorrect documentation or work procedures.

Doing the right thing. Major resignalling projects can involve carrying out difficult work in hazardous working conditions. Human factors play a major part in installation and maintenance activities. *Photo Network Rail.*

- The use of inadequate or unsuitable test equipment, because the right equipment is not available; again to avoid delays.
- Test equipment or wire links which remain unintentionally in place after test/fault diagnosis.
- Performing defined testing only in part (e.g. due to time constraints or because the work is thought to be 'simple').

Issues particular to the interface between maintainer and signaller:

- Misinterpretation of information provided (e.g. too late/early, the wrong line/track/location etc.) – this was a primary motivation for the introduction of formalised communication and the use of the phonetic alphabet.
- Not, or wrongly, performing actions in response to a maintainer request (e.g. to prevent switch moving due to local work).
- Ignorance of declaration/communication of temporary safety relevant restriction/procedures.
- Not knowing of temporary safety relevant restrictions or operating procedures in place (e.g. transfer to the next signaller).

Maintenance example - the control of turnouts/points

Many different circuits are used for point control ranging from 4 up to 7 wire connections per motor. Each system has some disadvantages. As an example, the German 4-wire control of a standard turnout (which has external locking, mechanical internal control of the blade position, and sometimes includes blade detection devices) requires a safety check after any change within the wiring. This includes a so called 'position test', which is mandatory, in order to check if the physical position of the turnout matches with the position of the point control unit within the interlocking. Evidence shows that there have been missing or wrongly undertaken tests, which have led to accidents or near accidents. It is questionable whether this relatively cheap point control (only four wires for some kilometres) justifies the risk, given the dependence on fallible human testing.

Another related example from the UK relates to the remaking of the cable termination of a point machine, due to insulation degradation/damage. The work was viewed as simple and a full correspondence test was not done even though the rules require one. Unfortunately, the 20+ year old installation had a double fault situation, created by reversing the connection at the interlocking end to obtain correct functionality rather than correcting incorrect core numbers at the point end. This minor maintenance task resulted in the first train of the day being routed into a siding (fortunately without any further consequences other than the maintainers involved being prosecuted and fined for health and safety offences). It demonstrates that a required correspondence check is also there to protect against past errors.

It is human nature to cut corners if a task is considered simple or familiar. The old saying 'familiarity breeds contempt' can be very true.

Lessons learned: so what do all of these examples teach us?

Multiple equipment conventions sometimes coupled with new system developments, will always create risk at interfaces, AWS being a prime example. A thorough impact analysis on adjacent systems and end to end processes is vital when anything is changed in a complex technical and operational environment. Different suppliers with different conventions to achieve the same end result, may result in hidden consequences buried way down in the lower levels of system operation.

Many trains are fitted with multiple signalling systems for operation on both high speed and conventional lines, and across national borders, but the transition between these needs to be considered from a human factors perspective both in normal operation and partial failure conditions. The transition to another system after a period of consistent operation needs careful control and mitigation against repetitive behaviour, low workload issues and distraction. Examples include the Morpeth curve in the UK where a significant permanent speed reduction occurs in the middle of an otherwise high speed section leading to three major derailments between 1969 and 1994 (a TPWS speed trap has now been installed), and the Santiago de Compostela derailment in Spain in July 2013 occurring because a significant PSR was missed near the entry to a conventional line after a period of sustained high speed running on new infrastructure, with the legacy ASFA system offering no speed control or enforcement.

Another aspect of human behaviour which emerged from the UK Southall inquiry relates to why the ATP system present was not used. At that time the ATP system was in pilot trial mode and not in operation on a continuous basis. Whilst the driver concerned had been trained in its operation, he had not used the system for some time and in evidence, said he was not confident to use it. This perverse logic means he was more comfortable to drive a train at 200 km/h with no protection system at all than risk a reliability issue with a system he did not yet feel wholly familiar with. Humans often over or under estimate their own capabilities. During the ATP pilots there were examples of equipment deliberately being damaged, with some drivers saying the imposition of such a system was "an insult to their intelligence". Thankfully once the 'teething' problems were resolved, attitudes changed and drivers came to appreciate the support the system gives. In human factors terms, asking someone how comfortable or uncomfortable they feel about a particular task or about their workload overall is a useful piece of evidence to support analysis but should not be relied on in terms of determining whether a risk is tolerable.

Recommendations

Most major railway projects now include a requirement for human factors studies to be conducted and their results acted upon. However, this is often still an 'add-on'. Human factors approaches are inconsistent, lack cohesiveness and in some cases are still quite immature. Human factors knowledge and awareness is too concentrated within specialist teams and tends to focus on physical ergonomics with little consideration of the other elements. Human factors needs to be embedded into engineering, operational and maintenance processes and should be a consistent agenda item at project, design and gate reviews with appropriate expertise present to scrutinise the issues.

Human performance should never be taken as a given. Even the most diligent person is capable of making a mistake for a variety of reasons including unconscious behaviour and distraction. Systems therefore need to provide layered protection and risk assessments should be cautious in assuming that different issues cannot occur simultaneously.

All engineering and operations staff working in the industry should be trained in human factors awareness to the extent that they can recognise potential dangers and call in a specialist if the risks identified are potentially intolerable.

All companies and organisations working in the industry should either employ appropriate human factors specialists or have an arrangement with a human factors expert who can provide support.

An attitude persists in some places that '*we set rules and people must obey them; if they do not, then they are at fault* '. Many administrations still take a hard line when a human error is part of an accident or incident causation, quickly blaming and possibly prosecuting the individual. Safety management systems should always include provision for the collection and analysis of incidents involving human error in both normal and degraded operation, so as to identify and act upon the risks that make errors more likely or even inevitable. This should include monitoring automatic or fall-back systems being used inappropriately as a day to day measure to ease workload or maintain a train service. The Zs-1 Ersatzsignal is one example; another is constantly running against a service brake over-speed intervention level for an ATP system.

All material changes to systems or processes should include human factors as part of their impact assessment with a particular focus on interfaces, workloads (including workloads which are too low as well as too high), training, competence assessment and management. A particular emphasis should be placed on the interfaces between systems, seeking out potential hazards from learned or habitual behaviours in one system that might occur in the territory of another. Training and awareness alone may not be enough to mitigate these hazards, and sometimes it will be necessary to change system configurations or operational processes to improve barriers. The transition from automatic train operation (ATO) to manual driving on an adjacent section brings particular concerns and it is known that the RSSB human factors team is already working in this area.

Automatic systems are designed by humans and diligence is needed to maintain 'state of the art' testing and validation of such systems to reduce error rates. Error free software is a very rare commodity. Automatic testing and the use of formal methods can improve test coverage and in the future the structured use of 'self-learning' systems potentially offers new ways of ensuring that unsafe conditions are not created.

Managers need to better engage with employees and their representatives on human factors issues. Employers and employees must both act responsibly, with employers prepared to respond to real safety concerns with appropriate measures; and representatives not 'playing the safety card' by claiming safety issues where none exist, simply to protect jobs or status. The railway is entering a period where there is likely to be increased competition from autonomous road vehicles, and improvements in efficiency and increased automation are unavoidable. Work practices will change but maintaining a safe system and treating people fairly must be constant objectives. No one in the rail industry wants to see a return to contraction and closures.

The ITC trusts that this article will raise the overall knowledge and understanding of human factors in the rail industry. It is a vitally important subject area, the analysis and control or mitigation of which needs to permeate everything undertaken, particularly the management of change.